Brute Force und DOS

Absicherungen (nicht nur) der Session und des Logins in Stud.IP

André Noack (data-quest) & Jan-Hendrik Willms (Uni Oldenburg)

Problemstellung

- Viele Bereiche in Stud.IP sind abgesichert
  - XSS -> htmlReady()
  - SQL-Injection -> Prepared Statements
  - Passwörter -> Hashes

  - Brute Force -> ???

Betroffene Bereiche

- Login
  - Keine Einschränkung der Anmeldeversuche pro Zeitraum
- Session
  - Keine Einschränkung der Versuche des Session-ID-„Ratens“ pro Zeitraum
- JSONAPI
  - Keine Einschränkungen (Basic Auth, Session, OAuth)

Mögliche Lösungen

- Rate Limiting
- Wartezeit zwischen Versuchen kontinuierlich erhöhen
- Einschränkungen pro betroffenem Nutzer oder via IP?

- Performance?
- Auswirkungen auf Last?