IT Sicherheit

02 Übungen

AAA - Challenge-Response-Verfahren (1)

Bob hat Passwort in Plain-Text gespeichert

1. Bob erstellt eine Nonce und sendet es mit der gewünschten Hash-Funktion (SHA256) an Alice
2. Alice bildet die Hash-Funktion von Passwort und Nonce
3. Alice schickt den Hash
4. Bob vergleicht die beiden Hashes

AAA - Challenge-Response-Verfahren (2)

Bob hat Passwort als SHA256 gespeichert

1. Bob erstellt eine Nonce und sendet es mit der gewünschten Hash-Funktion (SHA256) an Alice
2. Alice bildet die Hash-Funktion von Passwort dann die Hash-Funktion vom gehashten Passwort und Nonce
3. Alice schickt den Hash
4. Bob vergleicht die beiden Hashes

AAA - Challenge-Response-Verfahren (3)

Bob hat Passwort als Salted SHA256 gespeichert

1. Bob erstellt eine Nonce und sendet es mit der gewünschten Hash-Funktion (SHA256) und dem Salt an Alice
2. Alice bildet die Hash-Funktion von Passwort und Salt, dann die Hash-Funktion vom gehashten Passwort und Nonce
3. Alice schickt den Hash
4. Bob vergleicht die beiden Hashes

AAA - Challenge-Response-Verfahren (4)

Bob akzeptiert die Response nur mit einem Timestamp, welcher nicht älter als 30 Sekunden ist

1. Bob erstellt eine Nonce und sendet es mit der gewünschten Hash-Funktion (SHA256) und dem Salt an Alice
2. Alice bildet die Hash-Funktion von Passwort und Salt, dann die Hash-Funktion vom gehashten Passwort und Nonce und dem aktuellen Zeitpunkt
3. Alice schickt den Hash und den verwendeten Zeitpunkt
4. Bob vergleicht die beiden Hashes und überprüft, ob der verwendete Zeitpunkt nicht älter als 30 Sekunden ist

SSO

- SAML Playground
  - https://www.samltool.com/generic_sso_req.php
- OIDC Playground
  - https://www.oauth.com/playground/client-registration.html