**Studiengang Informatik**
apsi 2021

**Fachhochschule Nordwestschweiz**
A. Wagner, M. Schläpfer, R. Wagner

## Lösungsblatt 13 — 10. Januar 2022

## Aufgabe 13-1: OAuth 2.0

(a) Misconfiguration und fehlerhafte Umsetzung im Umgang mit *access token* und *id token*. Mangelhafte oder fehlende Prüfung des access token und entsprechender Autorisierung. Mangelhafte oder fehlende Überprüfung, ob access und id token im gleichen Kontext ausgestellt wurden.

(b) Strikte Umsetzung gemäss RFCs, Verwendung von PKCE (siehe unten), Umsetzung Security Best Practices. Nachfolgende Slides geben hierzu einen guten Überblick:

`https://speakerdeck.com/leastprivilege/oauth-and-openid-connect-security-best-practices.`

Ein mögliches Angriffsszenario basiert auf den verwendeten redirects, welche dahingehend ausgenutzt werden könnten, dass der *authorization code* an eine andere App unter der Kontrolle des Angreifers gesendet werden könnte. Dies kann mittels *Proof Key for Code Exchange (PKCE)*, sprich "Pixy", verhindert werden. Das oben verlinkte Slidedeck zeigt ein Beispiel dazu auf Slide 29.

## Aufgabe 13-2: SAML 2

(a) Im Gegensatz zu *SP-initiated* SSO, löst bei *IdP-initiated* SSO der IdP den Login aus. Analog zu einem token login, wo bereits mit dem ersten Request ein token mitgeschickt wird. Der Benutzer authentisiert sich beim IdP und wählt dort einen Service. Beim Absprung auf den Service wird eine SAML 2.0 Assertion mitgesendet. Diese beinhaltet alle relevanten Informationen zum Kontext (Session, Benutzer).

(b) Da der aufgerufene Service die Authentisierung nicht initiiert, könnte eine gestohlene Assertion von einem Man-in-the-middle (MITM) verwendet werden. Möglichkeiten, dieses Risiko zu minimieren beinhalten eine möglichst kurze Gültigkeitsdauer der ausgestellten Assertions des IdP und Replay-detection beim SP.