

Übungsblatt 13

20. Dezember 2021

Aufgabe 13-1: OAuth 2.0

Lesen Sie das in der Vorlesung referenzierte Paper von Yang et. al. welches Sie im Übungsordner finden. Beantworten Sie dabei die folgenden Fragen.

- (a) Was ist das Hauptproblem in der Umsetzung, welches in diesem Angriffsszenario ausgenutzt wird?
- (b) OAuth 2.0 ist mittlerweile der de facto Standard bei Mobile Apps. Wie wird denn das Problem heute gelöst? Recherchieren Sie dazu im Internet.

Aufgabe 13-2: SAML 2

In der Vorlesung haben Sie gesehen, wie SP-initiated SSO mit SAML 2 funktioniert. Lesen Sie sich unter nachfolgendem Link ein und beantworten Sie anschliessend die Fragen.

<https://www.identityserver.com/articles/the-dangers-of-saml-idp-initiated-sso>

- (a) Wie funktioniert IdP-initiated SSO und was sind die Unterschiede zu SP-initiated SSO?
- (b) Beschreiben Sie die möglichen Sicherheitsprobleme mit IdP-initiated SSO und wie diesen zumindest teilweise begegnet werden kann.