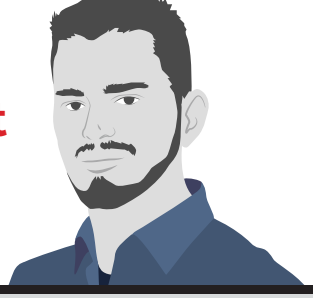
Single Sign-On Security: OAuth & OpenID Connect

IT-Security Training



Training Contents (2 DAYS)

Single Sign-On (SSO) procedures belong to the most important Internet technologies and are used by many applications. They allow to design the registration and login process as easy as possible for users and enable applications to be connected to social networks. OAuth and OpenID Connect are established as common standards today. However, serious attacks on SSO procedures have been discovered in recent years. These attacks exploit the complexity of the underlying standards, as well as implementation flaws, and allow attackers to authenticate themselves as arbitrary users or to access confidential user data. In this way, the data can be read, manipulated or deleted.

Due to the crucial role that single sign-on procedures fulfill in an application, it is essential to understand and address the problems of these technologies in detail. The training will address the following questions, among others:

- In which cases should I use OAuth, in which cases OpenID Connect?
- What are the differences between the various OpenID Connect Flows?
- Which attacks on SSO flows are there and how can they be prevented?

It is possible to extend this training to 3 days by adding further details or by adding SAML if desired.

Requirements

This training is designed for two groups: For developers who practically use Single Sign-On procedures based on OAuth and OpenID Connect. Further on, penetration testers and security researchers who want to learn how to evaluate the security of Single Sign-On procedures based on OAuth and OpenID Connect are addressed.

DAY 1

- Introduction to Single Sign-On
- OAuth and OpenID Connect Flows
  - Code Flow
  - Implicit Flow
  - Hybrid Flow
- Generic Attacks on SSO Procedures
  - XSS, Clickjacking, CSRF, Open/Covert Redirects
- First OAuth- and OpenID Connect-specific Attacks

DAY 2

- ID Token
  - Details & Attacks
- Single-Phase Attacks
  - ID Spoofing Attacks
  - Signature Bypasses
- Cross-Phase Attacks
  - Issuer Confusion
  - Malicious Endpoint Attacks
  - IdP Confusion
- Further Technologies
  - Device Flow, Native Apps & PKCE
- Secure Token Bindings
  - Mutual TLS
  - Holder-of-Key

Lecturer

Dr. Christian Mainka

Christian Mainka received his doctorate in 2017 with a thesis on web services and single sign-on. He is the co-founder of Hackmanit and since 2009 he has been dealing with security aspects in the context of data description languages, such as XML. He developed the first web service-specific penetration testing tool "WS-Attacker". Since then he has continuously improved and expanded the tool, such that it can be used to automatically survey a broad spectrum of known attacks on web services. In his dissertation, "On Message-Level Security" he analyzes the security of modern single sign-on systems such as SAML, OAuth and OpenID Connect and discovered numerous security vulnerabilities.

Contact

christian.mainka@hackmanit.de
www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum
Germany