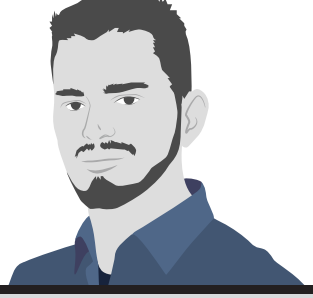
Web Service and Single Sign-On Security

IT-Security Training



Training Contents (2 DAYS)

Web services and single sign-on belong to the most important Internet technologies and enable you to provide your own services to third parties and connect them to social networks. In recent years, these technologies have become the target of serious attacks due to implementation flaws. The attacks take advantage of the complexity of the XML and single sign-on standards and allow an attacker to sensitive data from protected servers, authenticate as an arbitrary user or decrypt confidential data. Due to the importance of integrating web services and single sign-on into your enterprise ecosystem, it is important to understand and address the problems of these technologies.

The training will address the following questions:

- How do I use an XML parser correctly?
- How do I check an XML document's signature correctly?
- Which cryptographic algorithms should I avoid?
- Is encrypting of my messages with TLS sufficient?
- How can I protect my systems against attackers?

Requirements

This training is designed for two groups: For developers who practically use XML, web services and single sign-on systems. Further on penetration testers and security researchers are addressed who want to learn how to evaluate the security of those systems.

Do you use **OAuth** or **OpenID Connect**? Contact us for a single sign-on training on these specific topics.

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

DAY 1

- XML and SOAP based Web Services
- XML Schema and WS-Policy
- WS-Addressing and WS-Addressing Spoofing
- XML Parsing (DOM vs SAX)
- XML-specific Denial-of-Service Attacks
- XML Security and WS-Security
  - Differences to SSL/TLS
- XML Signature
  - ID- and XPath-based XML Signatures

DAY 2

- XML Signature Wrapping Attacks
- XML Encryption
  - Attacks on Symmetric Encryption
  - Attacks on Asymmetric Encryption
- Penetration Testing with WS-Attacker
  - SAML-based Single Sign-On Attacks
  - REST-based Web Services Attacks and Best Practices