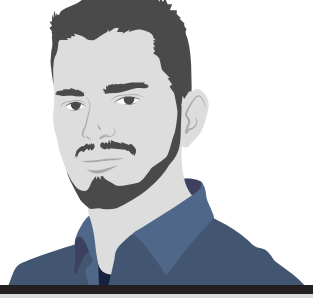
Single Sign-On Sicherheit: SAML

IT-Sicherheit Schulung



Schulungsinhalte

(2 TAGE)

Single Sign-On (SSO) Verfahren gehören zu den wichtigsten Internet-Technologien und werden von vielen Applikationen eingesetzt. Sie ermöglichen es die Registrierung und das Login für Benutzer möglichst einfach zu gestalten und Applikationen an soziale Netzwerke anzubinden. Der Einsatz von SAML ist hierbei weit verbreitet. In den letzten Jahren sind SSO Verfahren allerdings aufgrund von Implementierungsfehlern und Fehlern in den zugrundeliegenden Standards zum Ziel schwerwiegender Angriffe geworden. Die Angriffe nutzen die Komplexität der Standards aus und ermöglichen es Angreifern sich als beliebiger Benutzer zu authentisieren oder auf vertrauliche Daten der Benutzer zuzugreifen. Hierbei können die Daten ausgelesen, manipuliert oder gelöscht werden.

Durch die kritische Funktion, die Single Sign-On Verfahren bei dem Betrieb einer Applikation übernehmen, ist es wichtig, die Probleme dieser Technologien im Detail zu verstehen und zu adressieren. In der Schulung werden u. a. die nachfolgenden Fragen beantwortet:

- Wie verwende ich einen XML Parser richtig?
- Welche Arten von XML Signaturen gibt es für welchen Anwendungsfall?
- Wie validiere ich eine SAML Nachricht sicher?
- Wie schütze ich meinen Service oder Identity Provider vor bekannten Angriffen?

Voraussetzungen

Diese Schulung richtet sich an zwei Gruppen: Einerseits an Entwickler, die XML und SAML-basierte Single Sign-On Verfahren praktisch einsetzen; andererseits an Penetrationstester und Sicherheitsforscher, die sich mit dem Thema XML Sicherheit vertraut machen und Applikationen, die entsprechende SAML-basierte Single Sign-On Verfahren einsetzen, evaluieren möchten.

Dozent

Dr. Christian Mainka

Christian Mainka hat 2017 über die Themen Webservices und Single Sign-On promoviert. Er ist Mitgründer von Hackmanit und beschäftigt sich seit 2009 mit Sicherheitsaspekten die durch den Einsatz von Datenbeschreibungssprachen wie XML entstehen. Er hat das erste Webservice-spezifische Penetrationstest Tool „WS-Attacker“ entwickelt. Seitdem verbessert und erweitert er das Programm stetig, so dass es mittlerweile ein breites Spektrum der bekannten Angriffe auf Webservices vollautomatisch abdecken kann. In seiner Dissertation „On Message-Level Security“ analysiert er zudem die Sicherheit moderner Single Sign-On Verfahren wie SAML, OAuth und OpenID Connect und deckte zahlreiche Sicherheitslücken auf.

Kontakt

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

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum

TAG 1

- Einführung
  - XML und SOAP-basierte Webservices
  - XML Parsing (DOM vs. SAX)
  - XML Schema
- Document Type Definition
  - XML (External) Entity Angriffe
- XML-spezifische Denial-of-Service Angriffe
- XSLT
- XML Signature
  - ID-basierte und XPath-basierte XML Signaturen

TAG 2

- SAML-basiertes Single Sign-On
- Angriffe auf SAML Service Provider
  - Replay Angriffe
  - Signature Exclusion
  - XML Signature Wrapping (XSW)
  - Certificate Faking und Injection Angriffe
  - Covert Redirect Angriffe
- Angriffe auf SAML Identity Provider
- SAML Secure Bindings
- Erlerntes Wissen auf hauseigene Applikationen anwenden