**Praktikum / Bachelor- /Master-Arbeit**

# API Vulnerability Assessment

## Hintergrund der Arbeit

Für ein international agierendes Unternehmen aus der Automobil-Branche entwickelt die iC Consult verteilte Softwaresysteme, die im Bereich Identity- und Access-Management eingesetzt werden. Eine wichtige Komponente im Bereich der immer stärker vernetzten Anwendungen sind Web-Services, auf welche mittels Application Programming Interfaces (API) zugegriffen wird. Durch die immer komplexer werdenden Systeme erhöht sich die Angriffsfläche und das Bedrohungspotenzial für Hackerangriffe. Auch unterscheiden sich die Angriffsszenarien von denen einer typischen Web-Applikation.

## Ziel der Arbeit

Es sollen in einem ersten Schritt die wichtigsten Angriffsszenarien für API's (SOAP und REST) identifiziert werden.
Es sollen Möglichkeiten erarbeitet werden, wie Vulnerability Assessments (oder Penetrations-Tests) für API's durchgeführt werden können. Dabei soll auch der Fall im B2B Umfeld betrachtet werden, in dem auf eine API ausschließlich Zertifikatsgeschützt zugegriffen werden kann, wobei davon ausgegangen werden kann, dass das Client-Zertifikat dem Angreifer vorliegt.
Der Schwerpunkt der Vulnerability Assessments liegt dabei auf den oberen Schichten der Web-Services (Authentisierungs- und Autorisierungsverfahren, Web-Technologien, Applikations- und Service-Logik). Als weitere Aspekte sollen die Reproduzierbarkeit und Automatisierbarkeit der Vulnerability Assessments mit berücksichtigt werden.

Das verfolgte Ziel ergibt sich demnach aus der unmittelbaren Praxis und ist insgesamt in verschiedene Meilensteine unterteilt:

- Identifizieren der wichtigsten/wahrscheinlichsten Angriffsszenarien für Web-Services
- Evaluation geeigneter Werkzeuge und Hilfsmittel für die Durchführung von vulnerability-assessments für API's
- Definition des Umfangs des Vulnerability-Assessments
- Definition des Umfangs der Vulnerability-Assessment Tests
- Definition und Dokumentation der Vorgehensweise
- Durchführung der Vulnerability-Assessment Tests
- Dokumentation der Ergebnisse

## Anforderungen

Um einen schnellen Einstieg in die Thematik zu bekommen, sollten Interessierte die folgenden Anforderungen erfüllen:

iC Consult GmbH
Keltenring 14
82041 Oberhaching
www.ic-consult.de

Telefon: +49 89 660497-0
Telefax: +49 89 660497-19
USt.-Id.-Nr.: DE 186 893 020

Geschäftsführer :
Dipl.-Phys. Jürgen Biermann
HRB 116170 Amtsgericht
München

iC Consult Gesellschaft
für Systemintegration
und Kommunikation mbH

Commerzbank: BLZ 700 800 00
Konto-Nr.: 07 427 256 00
Deutsche Bank: BLZ 700 700 24
Konto-Nr.: 8889404

- Programmierkenntnisse in Java
- Kenntnisse in gängigen Web-Technologien und Protokollen (HTTP, SOAP, REST/Json, ...)
- Kenntnisse in Microsoft/Unix-basierten Betriebssystemen
- Methodisches Vorgehen
- Spaß an IT-Security

**Durchführung der Arbeit**

Die Meilensteine sind aufeinander aufbauend, d.h. es erfolgt eine Zwischenabnahme der verschiedenen Ergebnisartefakte. Die Arbeit wird eigenständig durchgeführt, es erfolgt eine inhaltliche und der Arbeit angepasste gekoppelte Betreuung durch einen Mitarbeiter der iC Consult GmbH. Die Betreuung ist an die jeweiligen Meilensteine gebunden. Entlang der definierten Meilensteine finden regelmäßige Treffen mit allen beteiligten Personen statt.

**Kontakt**

Bei Interesse, bitte wendet euch an:
iC Consult : www.ic-consult.de
Dr. -Ing. Nadina Hintz (nadina.hintz@ic-consult.de) Zettachring 8a, 70567 Stuttgart