Curriculum for

Certified Professional for Software Architecture (CPSA)®
Advanced Level

Module
WEBSEC

Web Security

Version 2020.1-EN; May 29, 2020

Table of Contents

The abbreviation "e. V." is part of the iSAQB's official name and stands for "eingetragener Verein" (registered association), which describes its status as a legal entity according to German law. For the purpose of simplicity, iSAQB e. V. shall hereafter be referred to as iSAQB without the use of said abbreviation.

This version of this document has been produced with comments (like this one) enabled. It is **NOT** intended for public distribution or publication, but primarily for internal iSAQB purposes.

List of Learning Goals

- LG 1-1: The is the first learning goal, in category xy
- LG 2-1: TBD
- LG 2-2: TBD
- LG 3-1: TBD
- LG 3-2: TBD
- LG 4-1: TBD
- LG 4-2: TBD
- LG 5-1: TBD
- LG 5-2: TBD
- LG 6-1: TBD
- LG 6-2: TBD

Introduction: General information about the iSAQB Advanced Level

What is taught in an Advanced Level module?

- The iSAQB Advanced Level offers modular training in three areas of competence with flexibly designable training paths. It takes individual inclinations and priorities into account.
- The certification is done as an assignment. The assessment and oral exam is conducted by experts appointed by the iSAQB.

What can Advanced Level (CPSA-A) graduates do?

CPSA-A graduates can:

- Independently and methodically design medium to large IT systems
- In IT systems of medium to high criticality, assume technical and content-related responsibility
- Conceptualize, design, and document actions to achieve quality requirements and support development teams in the implementation of these actions
- Control and execute architecture-relevant communication in medium to large development teams

Requirements for CPSA-A certification

- Successful training and certification as a Certified Professional for Software Architecture, Foundation Level® (CPSA-F)
- At least three years of full-time professional experience in the IT sector; collaboration on the design and development of at least two different IT systems
  - Exceptions are allowed on application (e.g., collaboration on open source projects)
- Training and further education within the scope of iSAQB Advanced Level training courses with a minimum of 70 credit points from at least three different areas of competence
  - existing certifications (for example: Sun/Oracle Java architect, Microsoft CSA) can be credited upon application
- Successful completion of the CPSA-A certification exam

Essentials

What does the module “WEBSEC” convey?

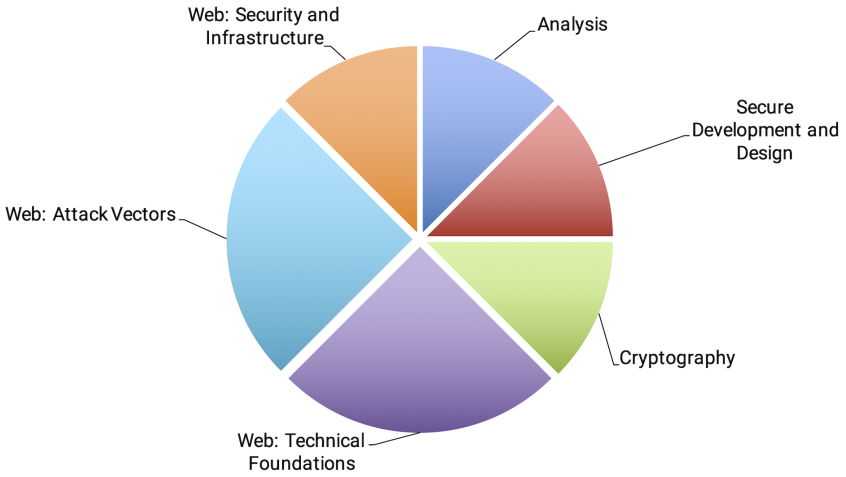
The module presents WEBSEC to the participants … At the end of the module, the participants know … and are able to …

Hier bitte das Modul bzw. dessen Lerninhalte zusammenfassend in 5-8 Sätzen beschreiben. Dabei `Web Security` nicht entfernen, beim Zusammenbauen wird dieser Platzhalter mit dem Modulnamen ersetzt.

Curriculum Structure and Recommended Durations

Content	Recommended minimum duration (minutes)
1. Analysis	180
2. Secure Development and Design	180
3. Cryptography	180
4. Web: Technical Foundations	360
5. Web: Attack Vectors	360
6. Web: Security and Infrastructure	180
Total	1440 (24h)

Allocation of time for the topic areas



Bitte sowohl die oben angegebene Tabelle als auch das beiliegende Excel-Dokument entsprechend anpassen und das Pie-Chart als "zeitaufteilung.png" nach `../images/01-basics` exportieren

= = =

Please adjust the table above as well as the excel document according to your curriculum and export the pie chart as "chronological_breakdown.png" to `../images/01-basics`.

Duration, Teaching Method and Further Details

The times stated below are recommendations. The duration of a training course on the WEBSEC module should be at least 2 days, but may be longer. Providers may differ in terms of duration, teaching method, type and structure of the exercises and the detailed course structure. In particular, the curriculum provides no specifications on the nature of the examples and exercises.

Licensed training courses for the WEBSEC module contribute the following credit points towards admission to the final Advanced Level certification exam:

Methodical Competence:	10 Points

Technical Competence:	20 Points
Communicative Competence:	0 Points

Prerequisites

Participants **should** have the following prerequisite knowledge:

- Prerequisite 1
- Prerequisite 2, etc.

Knowledge in the following areas may be **helpful** for understanding some concepts:

- Area 1:
  - Knowledge 1
  - Experience 2
  - Knowledge 3
  - Experience 4
  - Understanding 5

Kenntnisgruppen sowie Voraussetzungen bitte entsprechend ausformulieren!

Structure of the Curriculum

The individual sections of the curriculum are described according to the following structure:

- **Terms/principles**: Essential core terms of this topic.
- **Teaching/practice time**: Defines the minimum amount of teaching and practice time that must be spent on this topic or its practice in an accredited training course.
- **Learning goals**: Describes the content to be conveyed including its core terms and principles.

This section therefore also outlines the skills to be acquired in corresponding training courses.

Supplementary Information, Terms, Translations

To the extent necessary for understanding the curriculum, we have added definitions of technical terms to the iSAQB glossary and complemented them by references to (translated) literature.

1. Analysis

Duration: XXX min	Practice time: XXX min

1.1. Terms and Principles

- Term 1
- Term 2
- Term 3

Überschrift in 00-structure.adoc ersetzen

Sinnvolle Zeiten für Dauer und Übungszeit eintragen, vernünftige Begriffe aufzählen.

1.2. Learning Goals

LG 1-1: The is the first learning goal, in category xy

tbd.

2. Sicherer Entwurfs- und Entwicklungsprozess

Duration: XXX min	Practice time: XXX min

2.1. Terms and Principles

- Term 1
- Term 2
- Term 3

2.2. Learning Goals

LG 2-1: TBD

tbd.

LG 2-2: TBD

tbd.

3. Kryptographie

Duration: XXX min	Practice time: XXX min

3.1. Terms and Principles

- Term 1
- Term 2
- Term 3

3.2. Learning Goals

LG 3-1: TBD

tbd.

LG 3-2: TBD

tbd.

4. Web: Technische Grundlagen

Duration: XXX min	Practice time: XXX min

4.1. Terms and Principles

- Term 1
- Term 2
- Term 3

Überschrift in 00-structure.adoc ersetzen

Sinnvolle Zeiten für Dauer und Übungszeit eintragen, vernünftige Begriffe aufzählen.

4.2. Learning Goals

LG 4-1: TBD

tbd.

LG 4-2: TBD

tbd.

Die einzelnen Lernziele müssen nicht als einfache Aufzählungen mit Unterpunkten aufgeführt werden, sondern können auch gerne in ganzen Sätzen formuliert werden, welche die einzelnen Punkte (sofern möglich) integrieren.

5. Web: Bekannte Angriffe und Angriffsvektoren

Duration: XXX min	Practice time: XXX min

5.1. Terms and Principles

- Term 1
- Term 2
- Term 3

5.2. Learning Goals

LG 5-1: TBD

tbd.

LG 5-2: TBD

tbd.

6. Web: Security und Infrastruktur

Duration: XXX min	Practice time: XXX min

6.1. Terms and Principles

- Term 1
- Term 2
- Term 3

Überschrift in 00-structure.adoc ersetzen

Sinnvolle Zeiten für Dauer und Übungszeit eintragen, vernünftige Begriffe aufzählen.

6.2. Learning Goals

LG 6-1: TBD

tbd.

LG 6-2: TBD

tbd.

References

This section contains references that are cited in the curriculum.

Aufbau eines Eintrags-Ankers:

```
- [[[label,Text der erscheint]]]
```

ACHTUNG: Die Labels dürfen nur Buchstaben beinhalten, keine Zahlen oder Sonderzeichen

= = =

Structure of an anchor:

```
- [[[label,text that will be shown]]]
```

ATTENTION: labels have to be non-numeric.

A

- [Anderson 2001] Ross Anderson: "Security Engineering", O'Reilly 2001, Methodology

B

- [BSI Grundschutz] BSI IT-Grundschutz: "Umfassende Ein- und Ausgabevalidierung bei Webanwendungen und Web-Services", https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04393.html

C

- [CERT] CERT: "Top 10 Secure Coding Practices", https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices

F

- [FIRST] FIRST, Common Vulnerability Scoring System, https://www.first.org/cvss

M

- [McGraw 2006] Garry McGraw: "Software Security - Building Security in", Addison Wesley 2006
- [Mitnick 2002]Kevin Mitnick, Steve Wozniak: "The Art of Deception", John Willey & Sons 2002

O

- [OWASP TM] OWASP Wiki: "Threat Modelling", https://www.owasp.org/index.php/Application_Threat_Modeling

- [OWASP RRM] OWASP Wiki: "Risk Rating Methodology", https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- [OWASP SCP] OWASP Wiki: "Secure Coding Practices", https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

S

- [Schneier 1996] Bruce Schneier: "Applied Cryptography", John Wiley & Sons 1996
- [Schneier 1999] Bruce Schneier (1999), https://www.schneier.com/academic/archives/1999/12/attack_trees.html
- [Security Patterns] Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, Sommerlad: "Security Patterns", “Integrating Security and Systems Engineering”, Wiley 2005