AppSec
Application security Labs

APPLICATION SECURITY

ON LINE TRAINING ACADEMY

BY APPSEC LABS

APPSEC LABS ACADEMY

APPLICATION SECURITY & SECURE CODING ON LINE TRAINING PROGRAM

AppSec Labs is an expert application security company serving as a center of excellence in the field of application security for hundreds of organizations around the globe

In order to provide a scalable, cost effective solution for companies wishing to improve developer's knowledge of Application Security, AppSec Labs has created a series of E –learning based application security courses

THE APPLICATION SECURITY E LEARNING ADDED VALUES:

COMPLIANCE –
Almost all regulations require security training for development teams -our e-learnings' provide a complete solution for complying with regulations such as PCI, HIPAA and ISO 270001 application security training requirements.

NEW EMPLOYEE TRAINING –
new comers to your team can get immediate access to the course and can be required to pass the training and acquire the security knowledge they need from the get go

KNOWLEDGE BASE FOR SECURE CODING BEST PRACTICES –
training is great but with our e learning solutions developers have FREE ACCESS to the e learnings for as long as you are licensed and can use the e learnings on the fly to help implement security best practices throughout work.

CERTIFICATION –
Following completion of all chapters the students will be directed to a final exam- once passing the final exam, the student will receive a completion certificate.

APPSEC LABS ACADEMY

E LEARNING ADVANTAGES

FLEXIBILITY -

Trainees can go through the training program at times that are comfortable for them, on the organizational level this is a major advantage because the training isn't confined to a rigid time and location enabling the organization to keep work processes running as usual without needing to cause employees loss of full work days.

REDUCED TRAINING TIMES -

traditional classroom methods are time consuming, E learning time is estimated to be a quarter of "live class room" time, meaning that each hour of E learning is equivalent to 4 hours of class room training.

REDUCTION OF TRAINING COSTS -

deployment of global training is a costly affair – transportation and accommodation of trainers, training cost per class and lost time of development teams make class room training a costly affair...

APPSEC LABS ON LINE COURSE CATALOG

APPSEC LABS OFFERS THE FOLLOWING COURSES IN E –LEARNING MODE:

Course Title	Target Audience	Duration
Fundamentals of Application Security – OWASP top 10	Developers, QA, System designers/architects, managers	90 - 120 Minutes
Secure Coding Fundamentals for developers of all technologies	Developers, QA, System designers/architects, managers	90 - 120 Minutes
Java Secure Coding	Java Developers	5 - 6 hours
NET Secure Coding	Net Developers	5 - 6 hours
Android Secure Coding	Android Developers	3 - 4 hours
iOS Secure Coding	iOS Developers	3 - 4 hours
HTML5, JS & Angular Secure Coding	HTML5, JS & Angular Developers	90 -120 Minutes
Exclusive!!!! Android Application Hacking – BlackHat Edition	Security experts, penetration testers	6-7 hours

All our trainings include:

- Audio Lectures and presentations
- Demo / simulation videos
- Detailed explanation
- Searchable content
- Final exam
- Certification
- Personal VM for hands on labs available for some courses

TRAINING PLATFORM – APPSEC LABS ACADEMY LMS

All our trainings are performed via usage of the APPSEC LABS ACADEMY LMS which manages all courses, students and trainers and of course our hands-on labs.

HANDS-ON LABS & VIRTUAL MACHINES

In order to minimize the gap between academic knowledge and the real world, we have developed a unique cloud-based environment. This enables our students to practice what they learned in our course and gain hands-on experience.
Each student will get access to a personal virtual machine fully loaded for performing the exercise labs.

THE APPLICATION SECURITY AUTHORITY
Success stories by AppSec
GLOBAL CENTER OF EXCELLENCE IN APPLICATION SECURITY

JAVA
Secure
Coding

JAVA SECURE CODING

Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods , analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your J2ee applications.

The methodology of the Cycle of knowledge is as follows: Understand, Identify, Prevent. This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

The courses cover major security principles in the Java framework, the training includes programming vulnerabilities, and specific security issues relevant to J2EE web, JNLP applications.

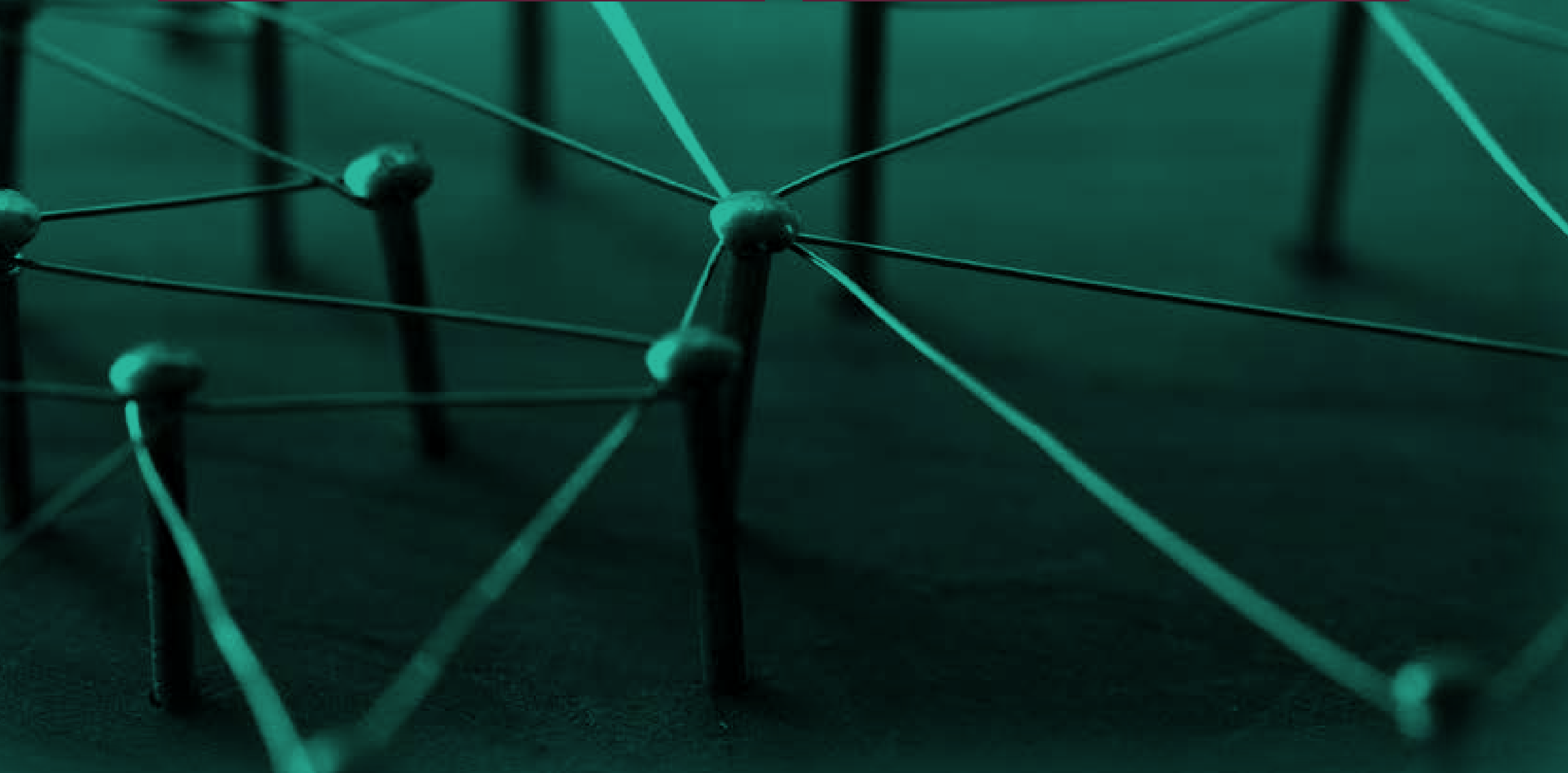
COURSE CHAPTERS
Unit 1: Introduction
Unit 1 Appendix: Tools
Unit 2: Input Validation
Unit 3: Authentication
Unit 4: Authorization
Unit 5: Session & Cookie Management
Unit 6: Dealing with Databases

COURSE CHAPTERS
Unit 7: Output Encoding
Unit 8: Error Handling
Unit 9: Security Logging
Unit 10: File Handling
Unit 11: File Uploads
Unit 12: Data Confidentiality and Integrity

TARGET AUDIENCE Java Developers

DURATION - 5-6 hours

OPTIONAL - personal VM access for labs.



.NET SECURE CODING

Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods , analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your. Net applications.

The methodology of the Cycle of knowledge is as follows: Understand, Identify, Prevent. This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

The courses cover major security principles in the .NET framework, the training includes programming vulnerabilities, and specific security issues relevant to .NET applications.

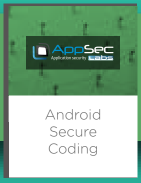
COURSE CHAPTERS
Unit 1: Introduction
Unit 1 Appendix: Tools
Unit 2: Input Validation
Unit 3: Authentication
Unit 4: Authorization
Unit 5: Session & Cookie Management
Unit 6: Dealing with Databases

DURRATION - 5-6 HOURS

COURSE CHAPTERS
Unit 7: Output Encoding
Unit 8: Error Handling
Unit 9: Security Logging
Unit 10: File Handling
Unit 11: File Uploads
Unit 12: Data Confidentiality and Integrity

TARGET AUDIENCE NET Developers

OPTIONAL - personal VM access for labs.


Android
Secure
Coding

ANDROID SECURE CODING

Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods, analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting **secure coding best practices** in order to bullet-proof your Androids applications.

The methodology of the Cycle of knowledge is as follows: **Understand, Identify**, Prevent. This methodology **presents** the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

The courses cover major security principles for securing Android applications, the training includes programming vulnerabilities, and specific security issues relevant to Android applications.

COURSE CHAPTERS
Unit 1: Intro to Mobile Application Secure Coding
Unit 2: Intro to Android Application Security Model
Unit 3: Android Permission Model
Unit 4: Secure Communication - Traffic Analysis & Manipulation
Unit 5: Secure Cryptography
Unit 6: Authentication and Authorization
Unit 7: Secure IPC
Unit 8: Reversing and Runtime Hooking
Unit 9: Anti Reversing Techniques
TARGET AUDIENCE Android developers **DURATION - 3-4 hours**

iOS
Secure
Coding

iOS SECURE CODING

Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods, analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your iOS applications.

The methodology of the Cycle of knowledge is as follows: Understand, Identify, Prevent. This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

The courses cover major security principles for securing iOS applications, the training includes programming vulnerabilities, and specific security issues relevant to iOS applications.

COURSE CHAPTERS
Unit 1: IIntro to Mobile Application Secure Coding
Unit 2: IIntroto iOS Application Security Model
Unit 3: Secure Storage
Unit 4: Secure Communication
DURATION - 3-4 hours

COURSE CHAPTERS
Unit 5: Secure Cryptography
Unit 6: Authentication and Authorization
Unit 7: Reversing and Runtime Hooking
Unit 8: Anti Reversing Techniques
TARGET AUDIENCE iOS development team members

HTML5,
JS & Angular
Secure Coding

HTML5, JS & ANGULAR SECURE CODING

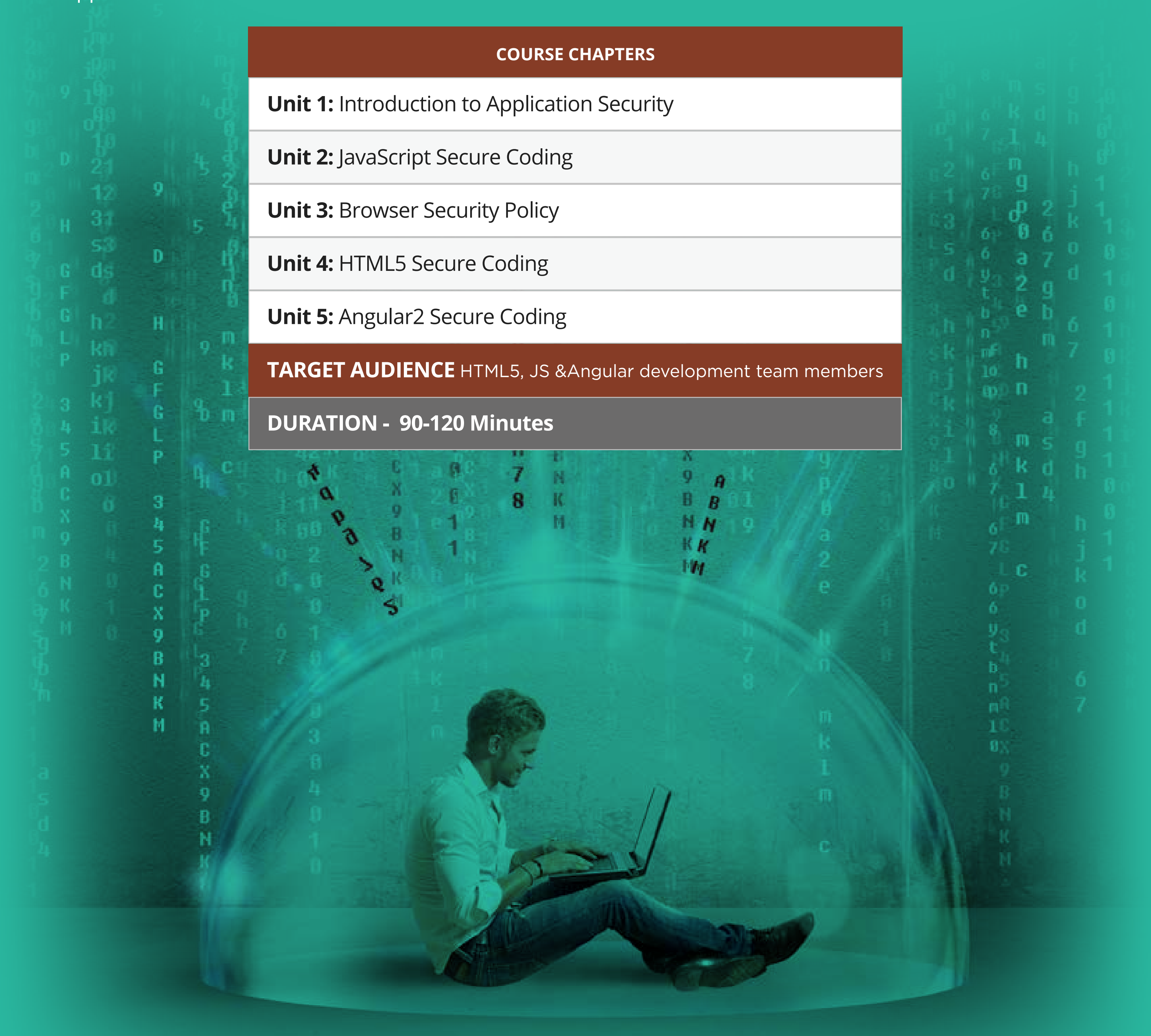
Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods, analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting secure coding best practices in order to bullet-proof your HTML5, JS and Angular applications.

The methodology of the Cycle of knowledge is as follows: Understand, Identify, Prevent. This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

The courses cover major security principles for securing HTML5, JS and Angular applications, the training includes programming vulnerabilities, and specific security issues relevant to HTML5, JS and Angular applications.

COURSE CHAPTERS
Unit 1: Introduction to Application Security
Unit 2: JavaScript Secure Coding
Unit 3: Browser Security Policy
Unit 4: HTML5 Secure Coding
Unit 5: Angular2 Secure Coding
TARGET AUDIENCE HTML5, JS &Angular development team members
DURATION - 90-120 Minutes



Secure Coding For Developers - Fundamentals

SECURE CODING FOR DEVELOPERS - FUNDAMENTALS

AppSec Application security Labs

Course abstract

Secure programming is the best defense against hackers. This multilayered course will demonstrate live real time hacking methods, analyze the code deficiency that enabled the attack and most importantly, teach how to prevent such vulnerabilities by adopting **secure coding best practices** in order to bullet-proof your applications.

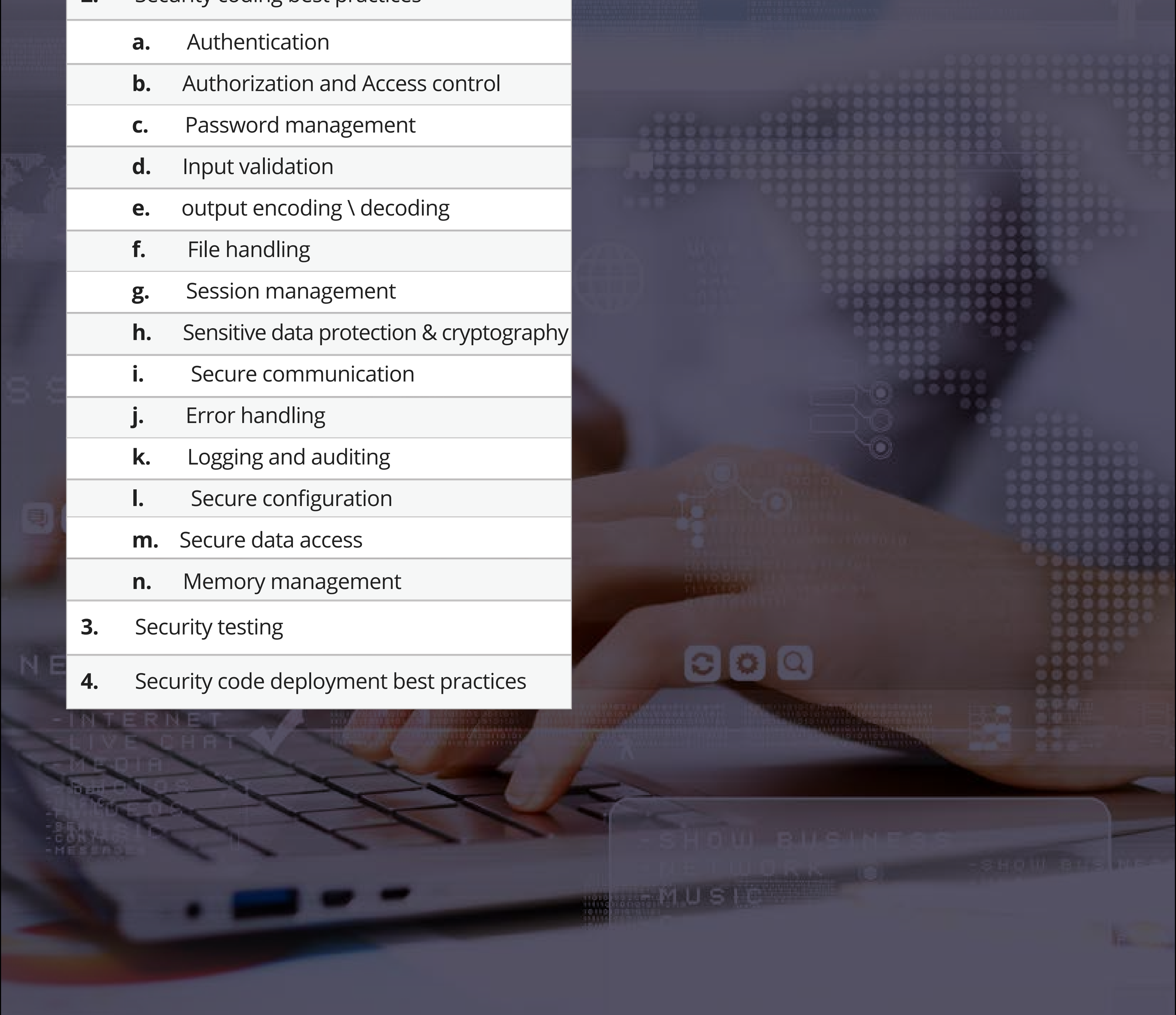
The methodology of the Cycle of knowledge is as follows: **Understand, Identify, Prevent.** This methodology presents the student with analytical tools to keep a deeper understanding of coding vulnerabilities and implement security countermeasures in different areas of the software development lifecycle.

TARGET AUDIENCE Developers of all languages

DURATION 90-120 Minutes

COURSE CHAPTERS

1. Security design best practices
2. Security coding best practices
    - **a.** Authentication
    - **b.** Authorization and Access control
    - **c.** Password management
    - **d.** Input validation
    - **e.** output encoding \ decoding
    - **f.** File handling
    - **g.** Session management
    - **h.** Sensitive data protection & cryptography
    - **i.** Secure communication
    - **j.** Error handling
    - **k.** Logging and auditing
    - **l.** Secure configuration
    - **m.** Secure data access
    - **n.** Memory management
3. Security testing
4. Security code deployment best practices



Fundamentals
of
Application
Security

FUNDAMENTALS OF APPLICATION SECURITY

Course abstract

This course is an introduction to application security threats, demonstrating the security problems that exist in corporate systems with a strong emphasis on application security and secure design.
This course covers the major security vulnerabilities including the OWASP top 10 vulnerabilities, and secure-design & coding best practices when designing and developing web applications & server-based services.

This course's main objective is raising the awareness on the problems that might occur without secure coding practices. The training aims to teach software engineers their important role in the corporate effort to secure its systems, while utilizing information security best practices. The student will learn about the threat landscape and the controls he should use during the software development lifecycle.

COURSE CHAPTERS

Unit 1: Injection Flaws	**Unit 6:** Security Misconfiguration
Unit 2: Cross-Site Scripting (XSS)	**Unit 7:** Insecure Cryptographic Storage
Unit 3: Broken Authentication & Session Management	**Unit 8:** Failure to Restrict URL Access
Unit 4: Insecure Direct Object References	**Unit 9:** Insufficient Transport Layer Protection
Unit 5: Cross-Site Request Forgery (CSRF)	**Unit 10:** Unvalidated Redirects & Forwards

TARGET AUDIENCE Developers, QA teams, System Architects, Managers

DURATION: 90-120 Min

The materials are presented in the following methodology:
Definition, Impact, Example Scenarios, Demo Video, Counter measures

CONTACT US FOR A DEMO TODAY: INFO@APPSEC-LABS.COM

SOME OF OUR ON LINE ACADEMY CUSTOMERS

NCR

bank hapoalim

amdocs

Check Point
SOFTWARE TECHNOLOGIES LTD.

888
HOLDINGS

ForeScout