

Security-Ausbildung in einem Großunternehmen der Softwareindustrie - Erfahrungen und Herausforderungen

Volkmar Lotz

Program Lead Security&Trust, SAP Research



Agenda

Part I – Build Knowledge: Baseline Education

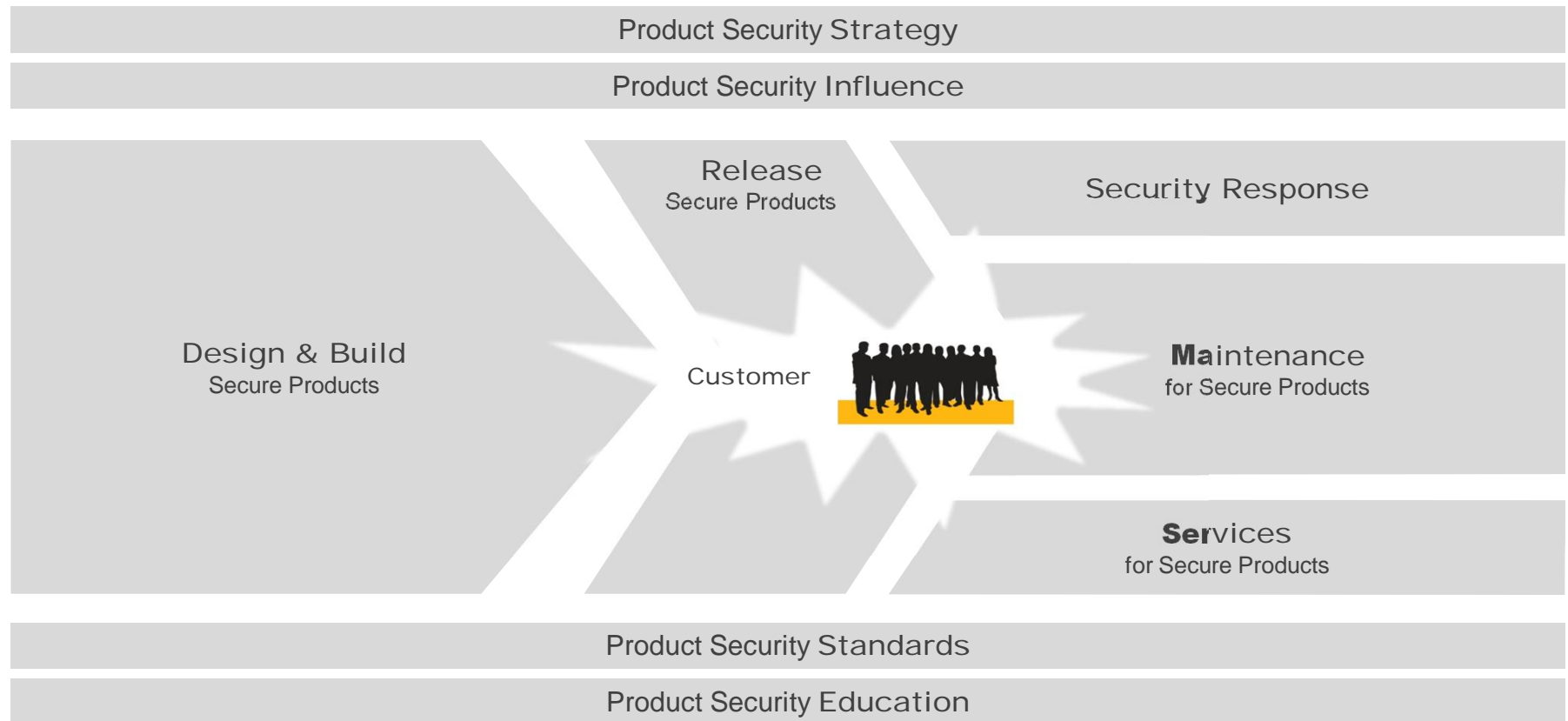
- Secure Programming Training as a Key Contribution to Product Security
- Training Content
- Training Formats
- Lessons Learned

Part II – Retain Knowledge: Refresh & Extend

- Extend: Specific Content
- Refresh: Keep Motivation High and Costs Low
- Gamification in 3 Steps
 - Microlearning
 - Entertainment
 - Progress
- Lessons Learned

Part I – Build Knowledge: Baseline Education

Product Security Lifecycle



Why Secure Programming Training at SAP Now (i.e., 2011)?

Increased exposure of data assets

- Cloud
- Mobile
- Business Ecosystems

Increased complexity and heterogeneity of technology

Increased attention of external security researchers

- Cf. security conference programmes
- SAP is no longer ignored by hackers

→ Technology frameworks and central groups are good, but do not fully substitute individual awareness and responsibility

Target Audience: Development-related Roles

- ABAP/Java/C++/... Developers
 - ABAP/Java/C++/... Development Architects
- } 3 day Secure Programming
-
- Security Experts in Development Groups
 - Solution Managers & Product Owners
 - Managers & Development Project Managers
 - Information Developers/ Technical Writers
 - (Security) Testers
 - Quality Managers
- } 1 day Secure Programming Awareness

Course Content

Unit 1 Introduction

Unit 2 Secure Programming

Unit 3 Security Testing

Unit 4 Identity and Access Management

Unit 5 Secure Development Life Cycle

Unit 6 Conclusion

Example Agenda for Classroom Training

Day 1

9:00 – 10:00

- Introduction

10:00 – 11:00

- Secure Programming

Break

11:30 – 12:30

- Secure Programming

Lunch

13:30 – 15:00

- Secure Programming

Break

15:30 – 17:00

- Secure Programming

Day 2

9:00 – 10:30

- Secure Programming

Break

11:00 – 12:00

- Secure Programming

Lunch

13:00 – 15:30

- Security Testing

Break

16:00 – 17:00

- Identity and Access Management

Day 3

9:00 – 10:30

- Identity and Access Management

Break

11:00 – 12:00

- Identity and Access Management

Lunch

13:00 – 14:00

- Security response

Training Formats

Classroom

Virtual Classroom

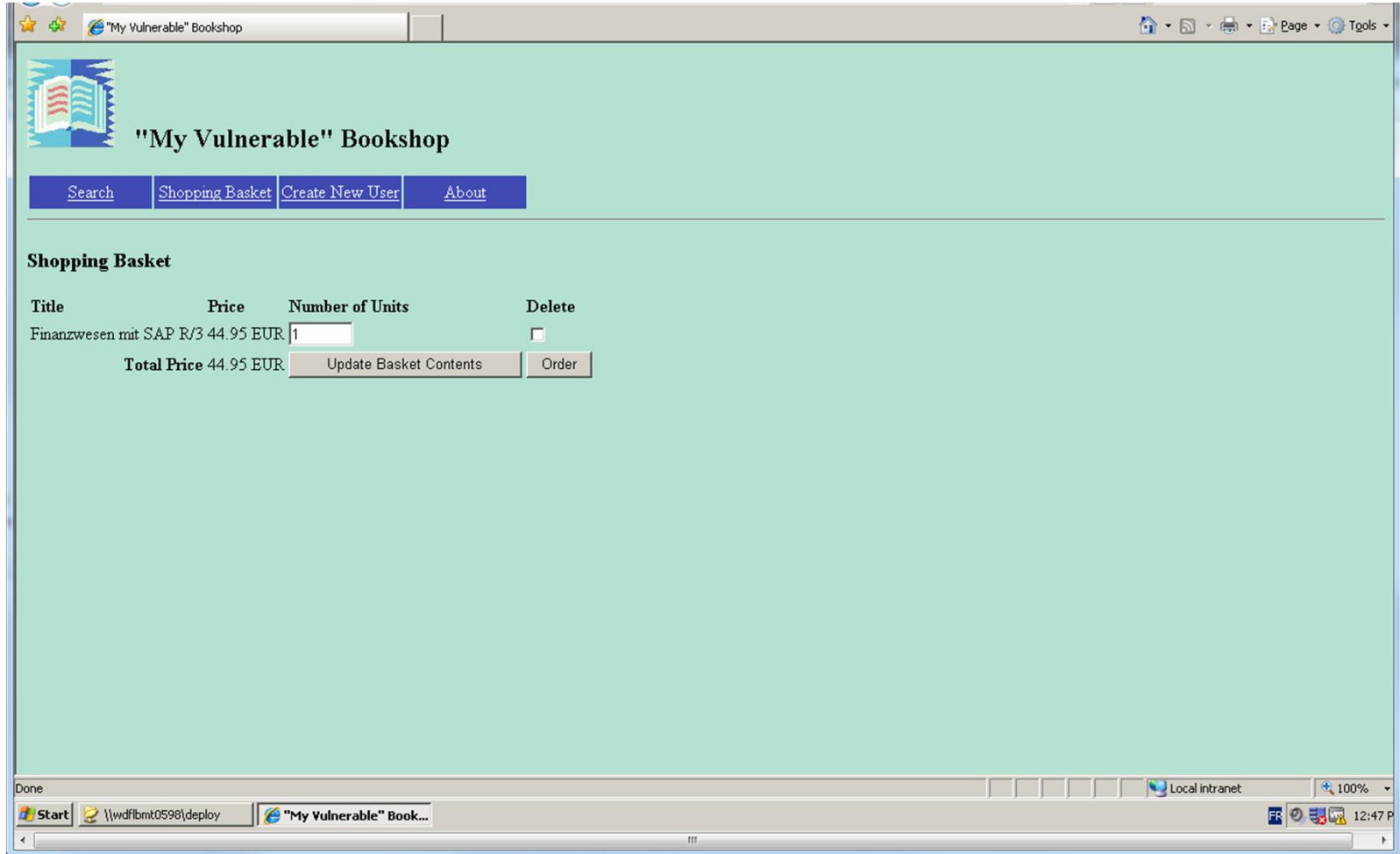
eLearning (1-day training only)

Web Assessment

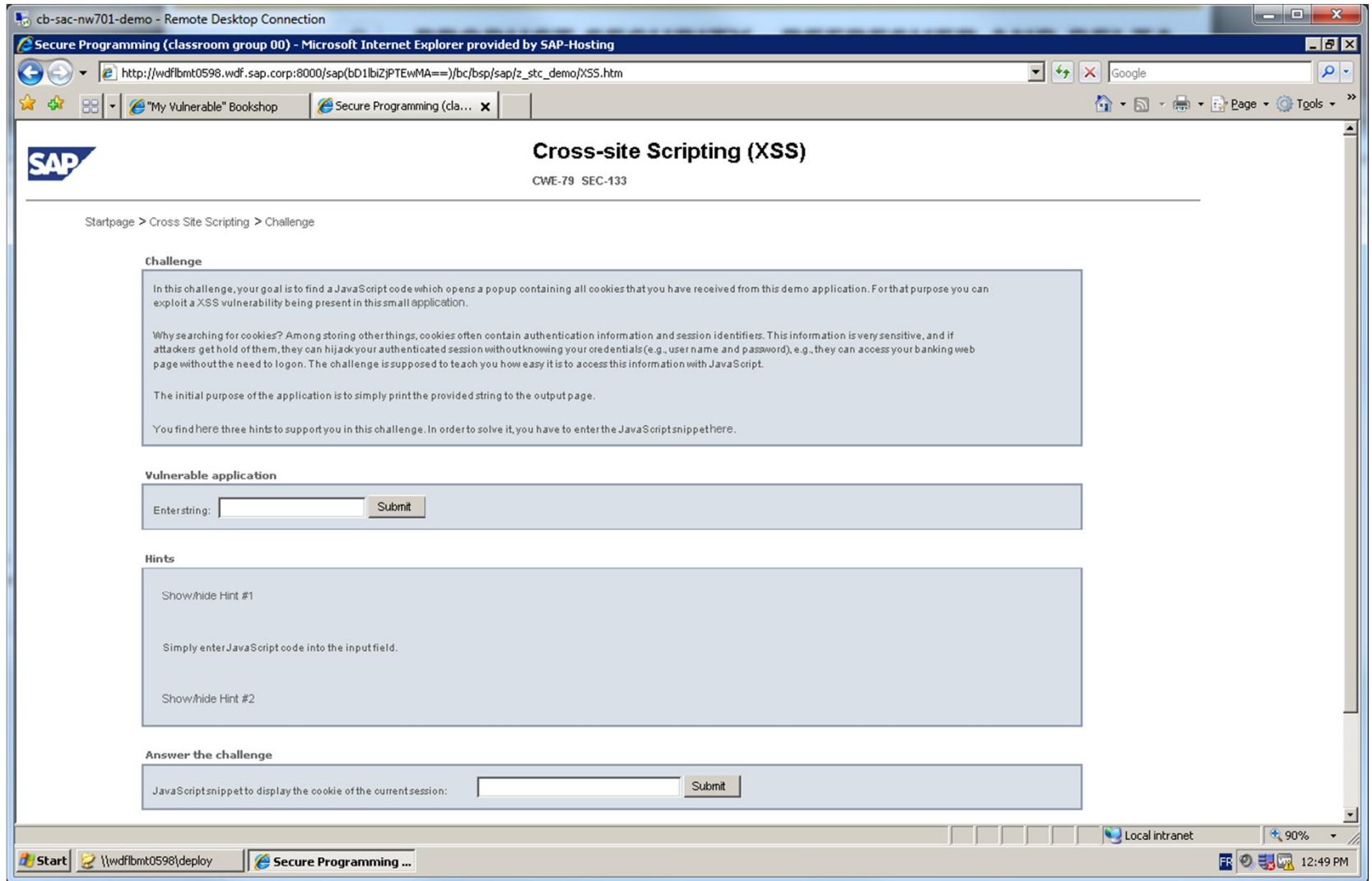
Community

Exercises in Lab Environment

Example Exercise (1): My Vulnerable Bookshop

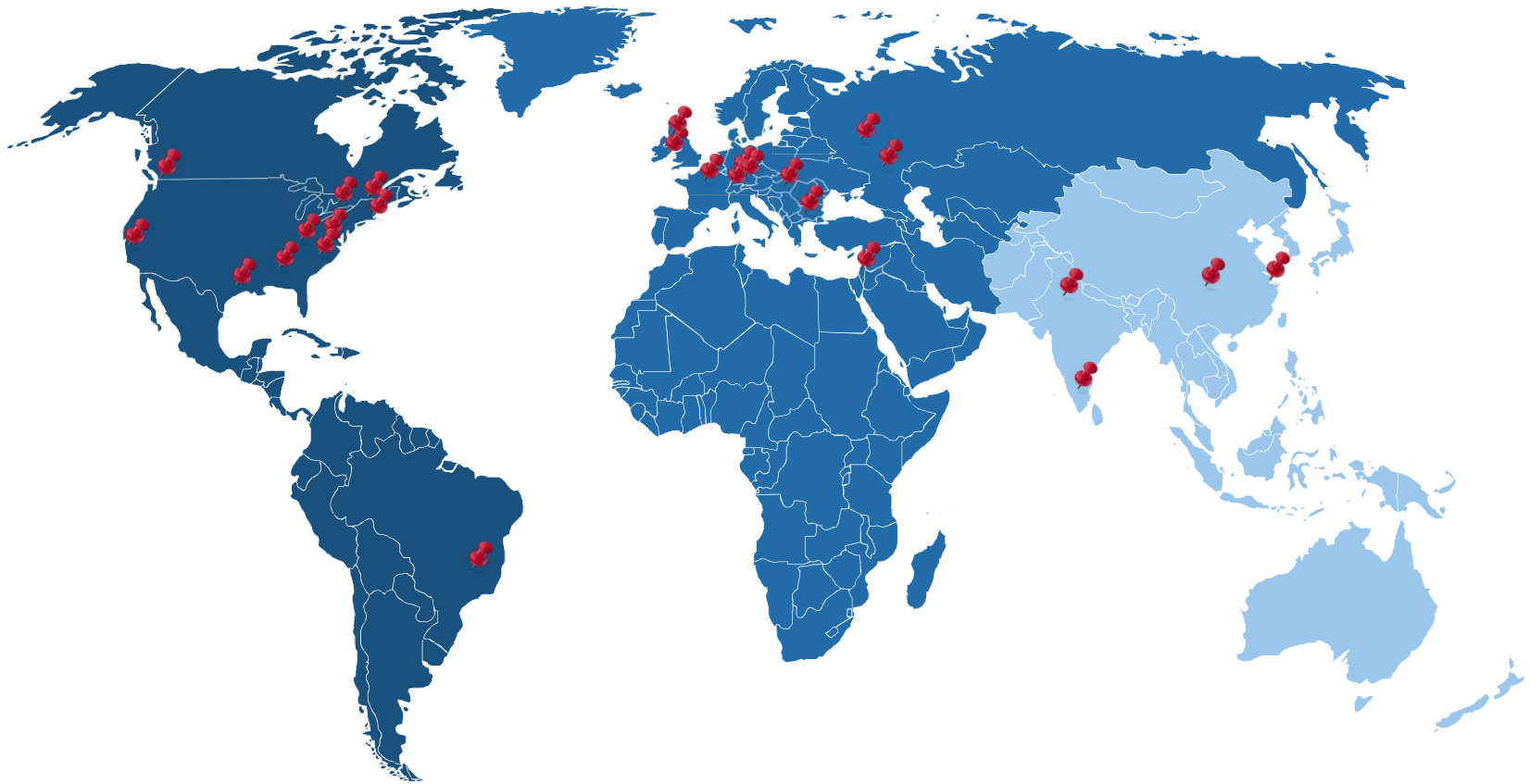


Example Exercise (2): XSS



SAP Product Security Training

16.000 attendees, ~600 classroom trainings, 35 locations, 75 trainers



Lessons Learned

“One size fits all” does not work

- Balance adaptation to specific context with effectiveness and costs
- SAP specific content
- Deal with contradicting feedback

Trainer role is critical

- Make them own the content
- Support through trainer community

Provide interactive content and different media

- Slides, pictures, videos, demos, training systems, ...
- Exercises, including those related to “dry topics”
- Hands-on approach

Run pilots (more than one)

Cultural specifics need to be considered

Put business units in charge

Part II – Retain Knowledge: Refresh & Extend

Extend: Special Topics

Specific topics addressed in separate modules:

- Frontend Security (e.g., HTML5)
- Database Security
- Mobile Security
- Requirements Engineering
- Threat Modelling
- Secure Architecture

Integration of security modules in general topic trainings

Refresh: Keep Motivation High and Costs Low

Virtual

Interactive

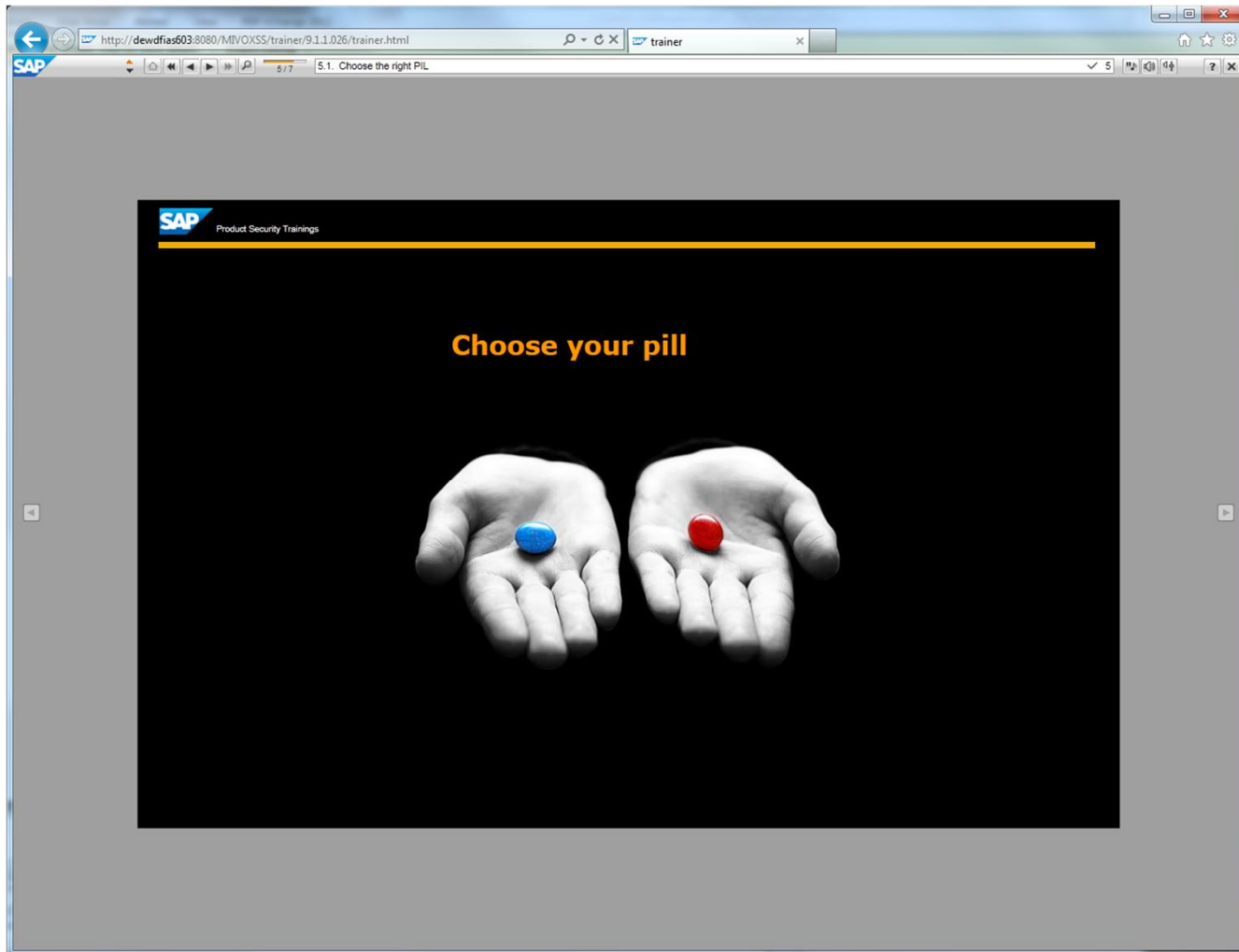
Self-controlled

Entertaining

Rewarding

→ Gamification

Leave the Choice



Definition

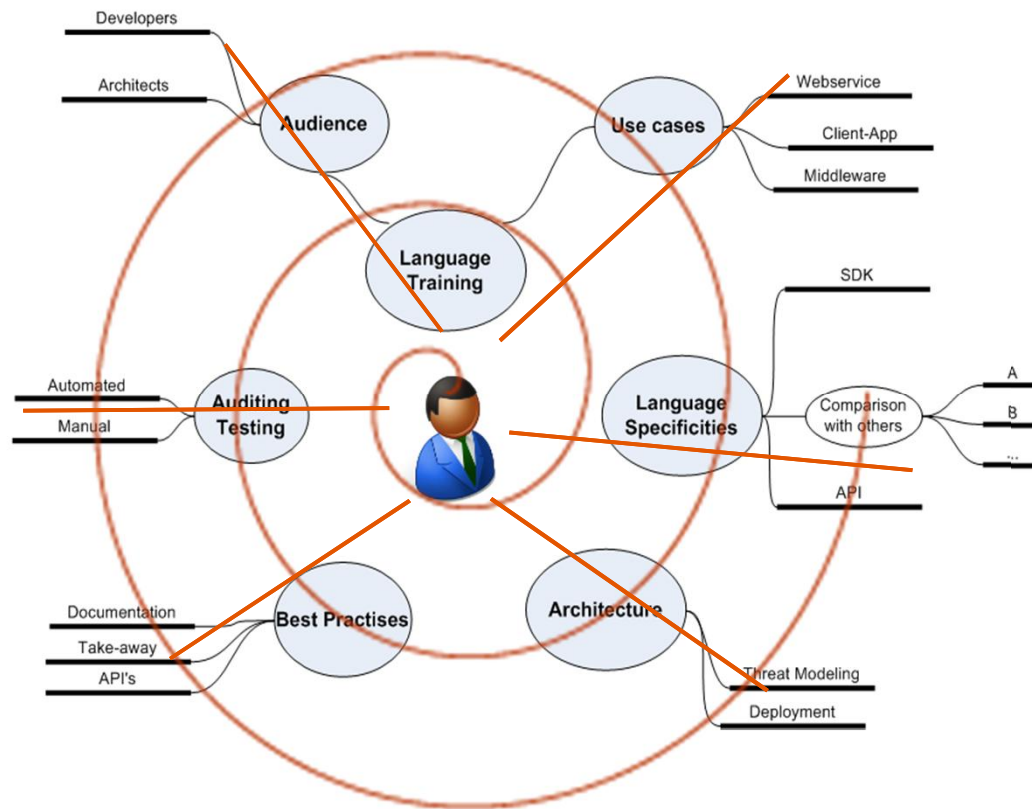
Enterprise Gamification & Serious Gaming

Gamification is “using game-based mechanics, aesthetics and game thinking to engage people, motivate action, promote learning, and solve problems.” ~ Karl Kapp

Serious Game is “a mental contest, played with a computer in accordance with specific rules that uses entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives.”
(wikipedia)

Gamification in 3 steps: 1st your need, your training

Personal Learning Environment: participant 's choice



- ➡ micro-learning
 - ➡ Small units (15mn)
 - ➡ Self contained

Example: Micro-learning

trainer - Microsoft Internet Explorer

https://iwdfvm4897/wpb/wa/1/~tag/published/trainer/9.1.2.211/trainer.html?startMode=start&assignmentId=C_C4D8CF27FC554C0F8ED13B32AE81D77B&show=book!BO_722BC3FB4E256291

SAP

6 / 7 2.1. Index

SAP Product Security Training

Leave the training

Product Standard Security **Secure Programming**

Product Security Response **Product Security Code Scans**

Diagram illustrating the structure of the training units, centered around a blue question mark icon, surrounded by orange concentric circles and icons representing different unit types (brain, question mark, factory, etc.).

Welcome
To see the description of each unit, click on these different types of icons:

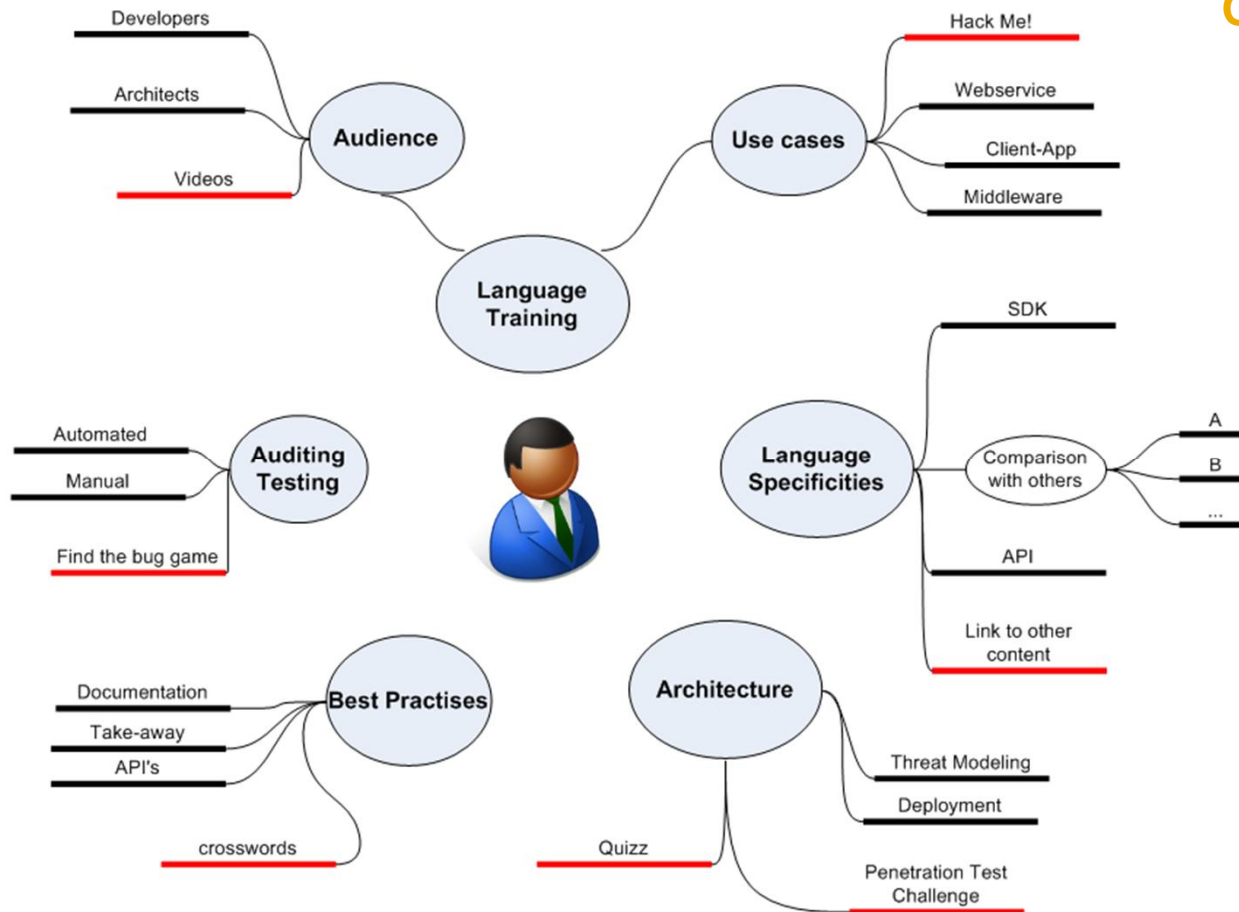
- Knowledge units are "must know"
- Practice units are "nice to know"
- Quizzes as another way to learn are "nice to know"
- Final unit to achieve the training

Then to start the unit, click on this button:

If you need support or want to give feedback, please join the [security learning community](#).

Gamification in 3 steps: 2nd raise the excitement

Interactivity and gamification on the content: making the content more attractive



Optional content

- ➡ Static or interactive
- ➡ Challenging
- ➡ Entertaining

Example: Storyboards



Example: Challenges

https://dewdfgw004548443/?show=book!BO_B0F6F4CC2DBE7EB5 - trainer - Microsoft Internet Explorer

SAP Product Security Training

Hacking Challenges

You can make SAP products more secure using multiple sources of information, for example: [secure programming guide](#), [secure programming training material](#) and the [security standard wiki \(most up-to-date\)](#).

Now, by clicking on the icons, you can try to exploit vulnerabilities on dedicated applications and get additional information.

To achieve these little hacks you can consult security training materials but the Internet will also give you very good hints.

SQL Injection

XSS

Buffer Overflow
(video)

Path Traversal

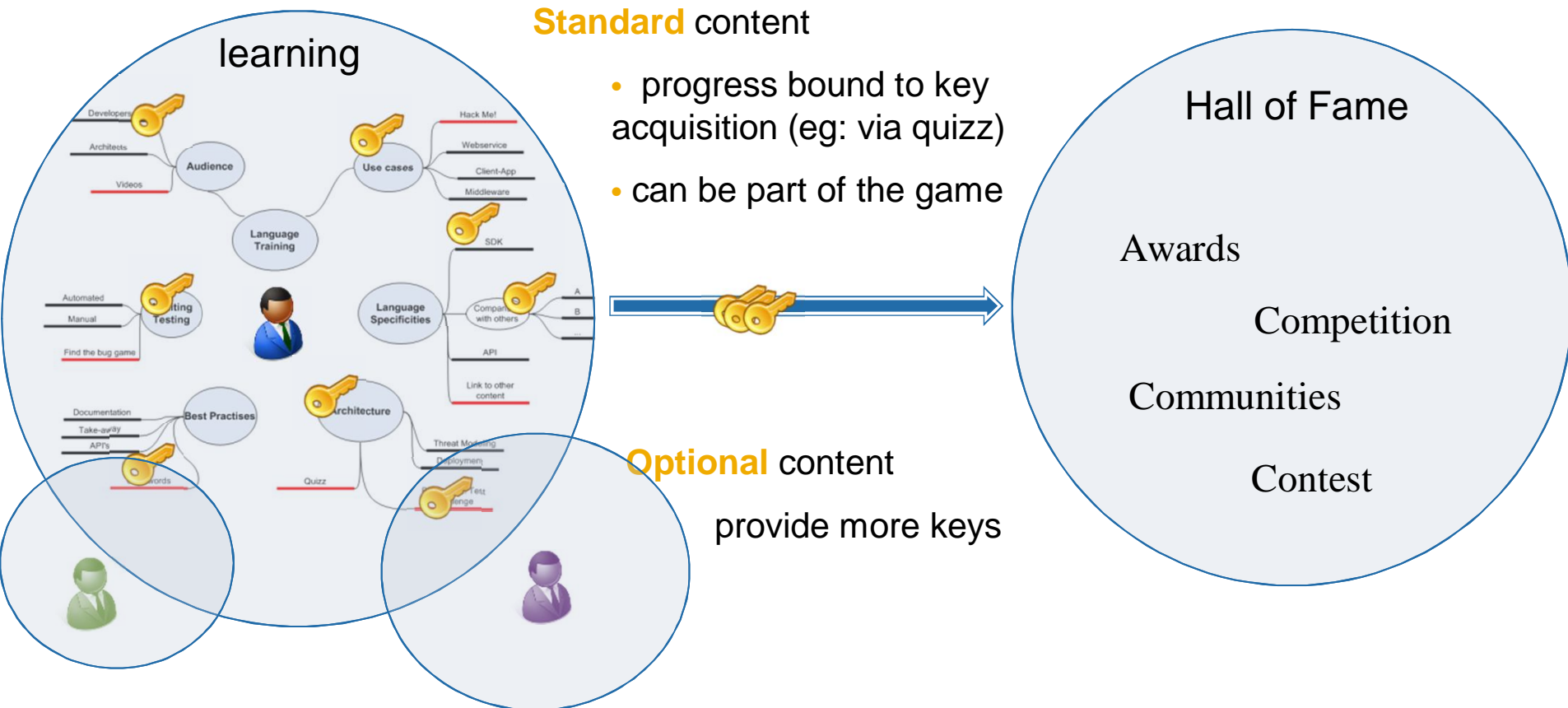
Password Cracking

Hacked!

Nearly Hacked!

Back to main index

Gamification in 3 steps: 3rd your progress is the KEY



Example: Achievements

The screenshot shows the 'My Achievements' view of the 'Security Refreshers 2012' page. The user is Paris Hilton. The page is titled 'PRODUCT SECURITY TRAINING'. It displays a list of achievements on the left, including Mobile Security, HTML5 Security, HANA Security, C# Secure Programming, ABAP Secure Programming, Java Secure Programming, and C/C++ Secure Programming. The main content area shows 'MY ACHIEVEMENTS' and 'RANK'. The user's rank is 'Padawan - 100pts' with a note 'Next: Knight at 400'. There are two achievement categories: 'Security Response' (Newbie, Expert) and 'Secure Coding' (XSS Newbie, XSS Expert). A 'POINTS HISTORY' graph is also visible.

The screenshot shows the 'Usage Details' view of the 'Security Refreshers 2012' page. The user is Paris Hilton. The page is titled 'SECURITY REFRESHERS 2012'. It displays a list of achievements on the left, including Mobile Security, HTML5 Security, HANA Security, C# Secure Programming, ABAP Secure Programming, Java Secure Programming, and C/C++ Secure Programming. The main content area shows 'LEVEL' and 'USAGE DETAILS'. The user's level is 'Expert' (Intermediate, Expert, Beginner). The usage details include 'Used since: Nov 5, 2012' and 'EVOLUTION'. A bar chart shows the user's progress in various security requirements: P/L Security Requirements, Code Scan, Secure Coding, and Security Response.

Take the Opportunity of Events

Product Security Summit

ANDROID CHALLENGE



Lessons Learned (so far)

Gamification approach is highly appreciated

- Across all cultures

... but leaving the choice is essential

Effort for technical realization required (limits of current products), but outweighed by savings in logistics and participant work time

Gamification is sensitive topic, close alignment with works council is mandatory



Thank You!