# 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

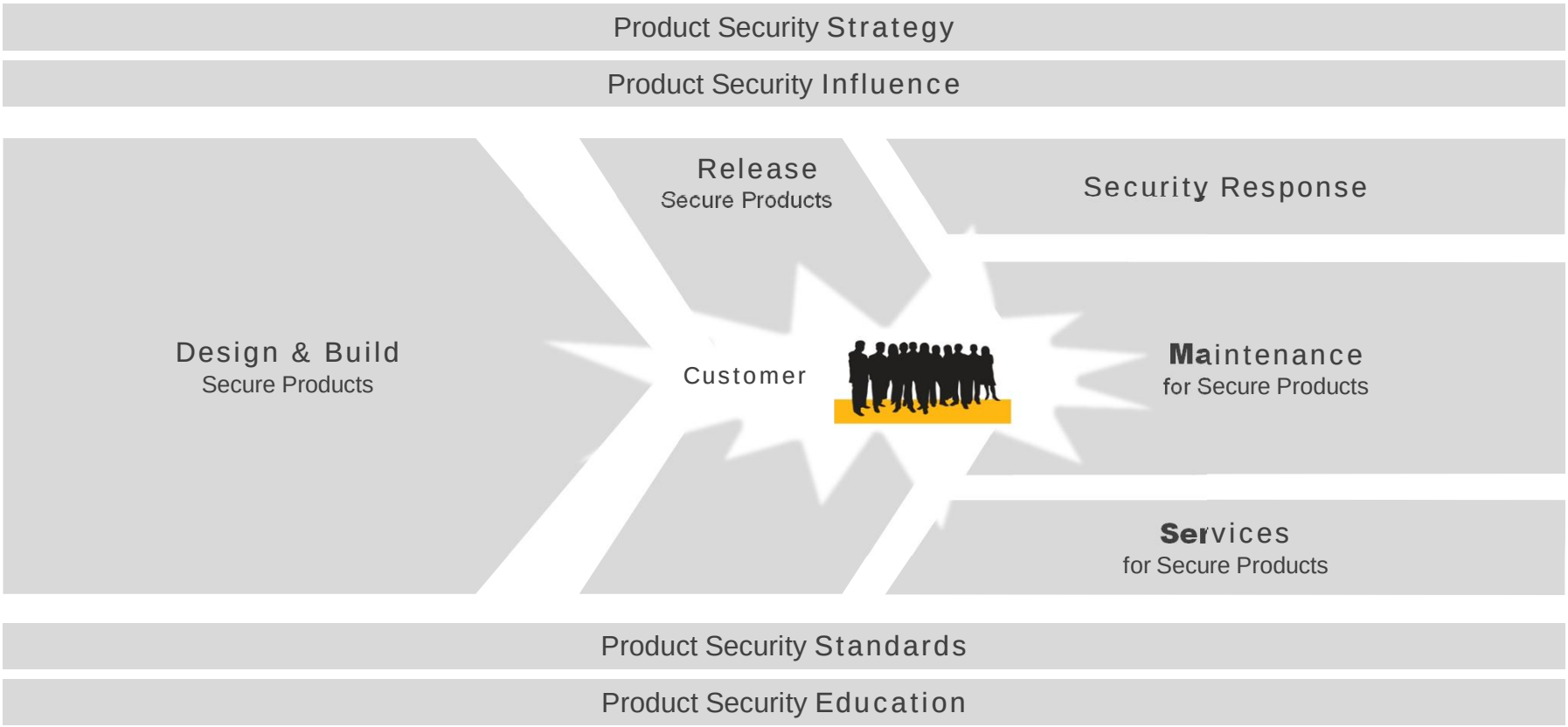
- Secure Programming Training as a Key Contribution to Product Security
- Training Content
- Training Formats
- Lessons Learned

## 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 reponsibility**

# 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

# 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**

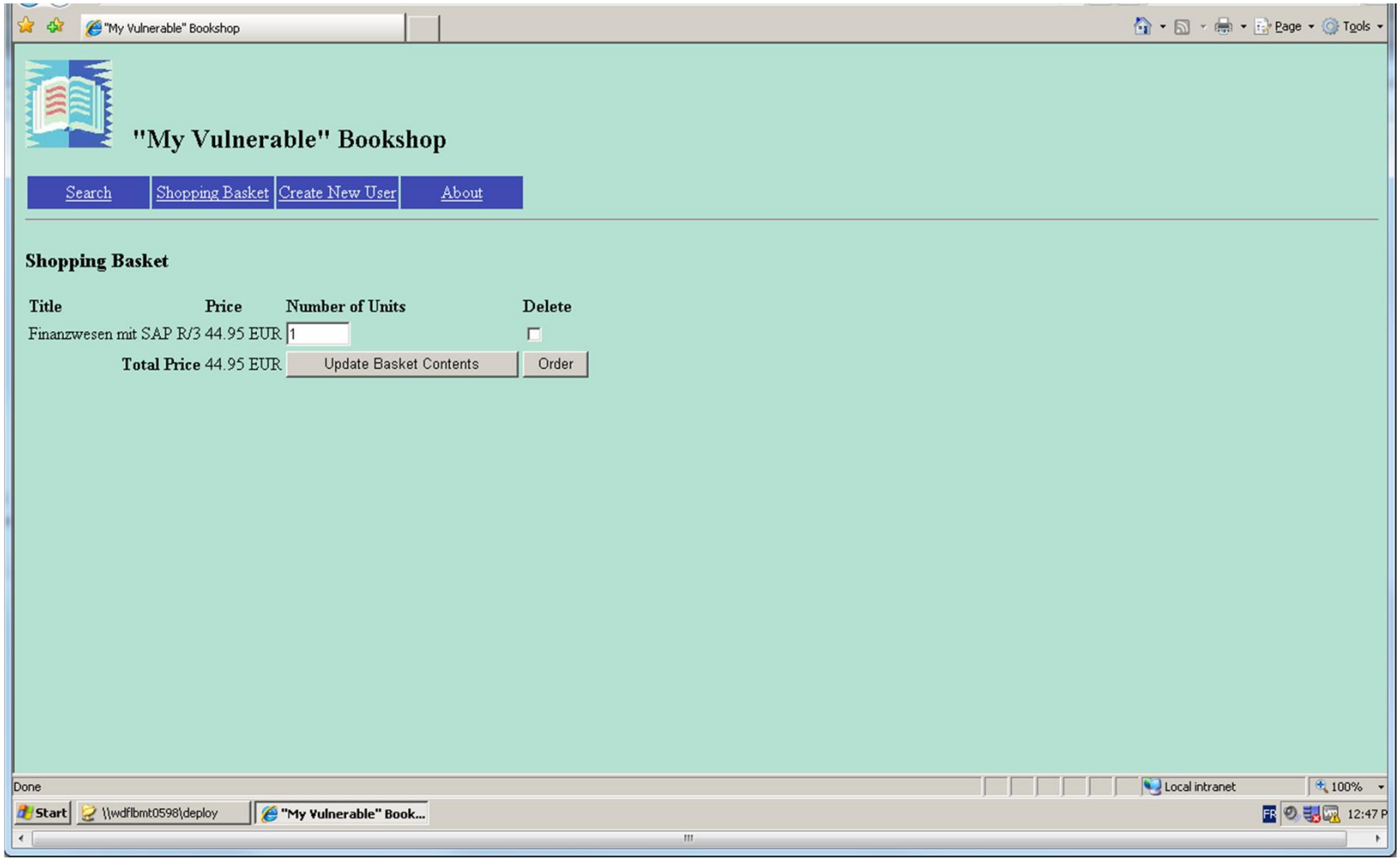
**eLearning (1-day training only)**

**Web Assessment**

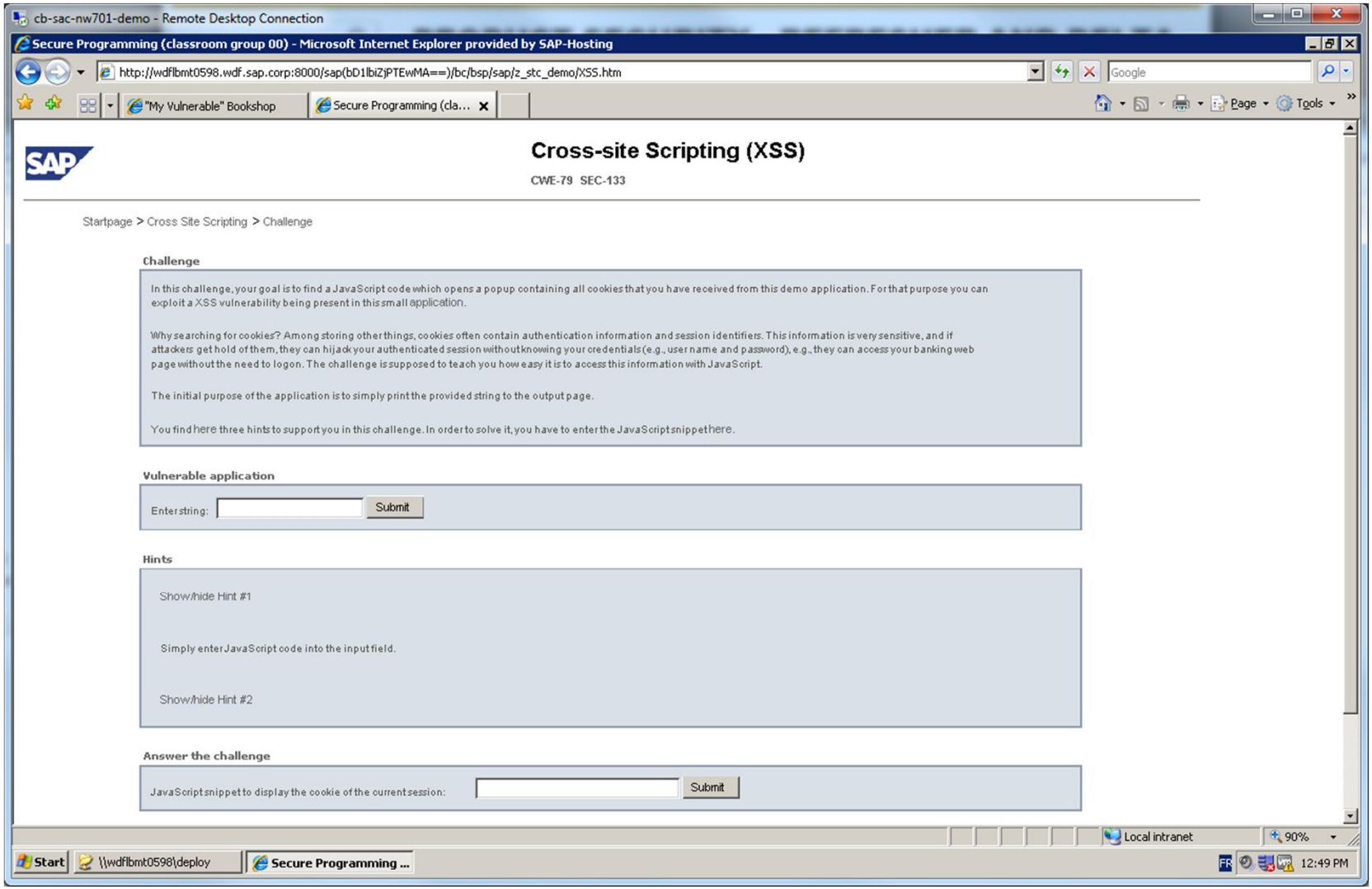
**Community**

**Exercises in Lab Environment**

# Example Exercise (1): My Vulnerable Bookshop

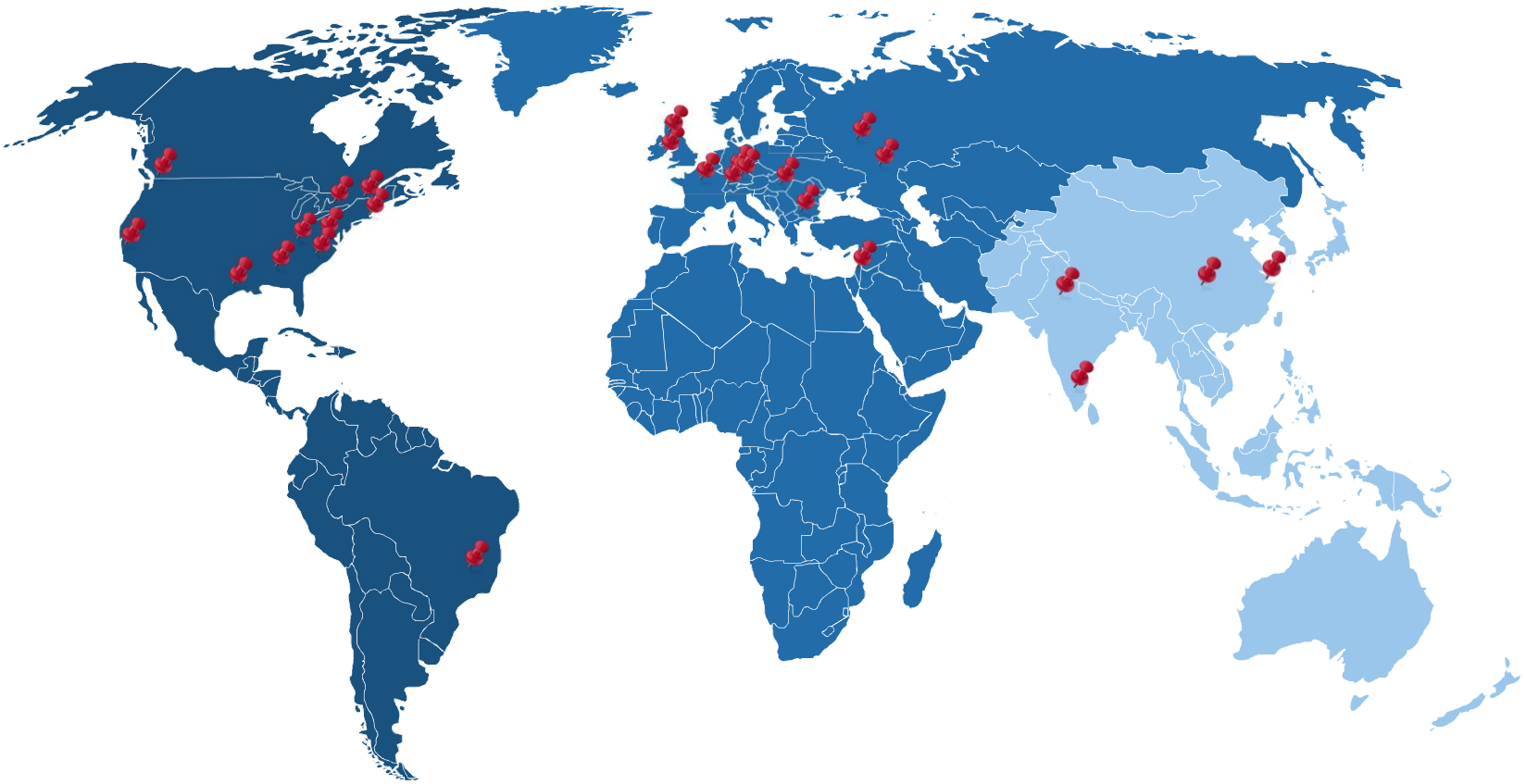


# Example Exercise (2): XSS



# 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**

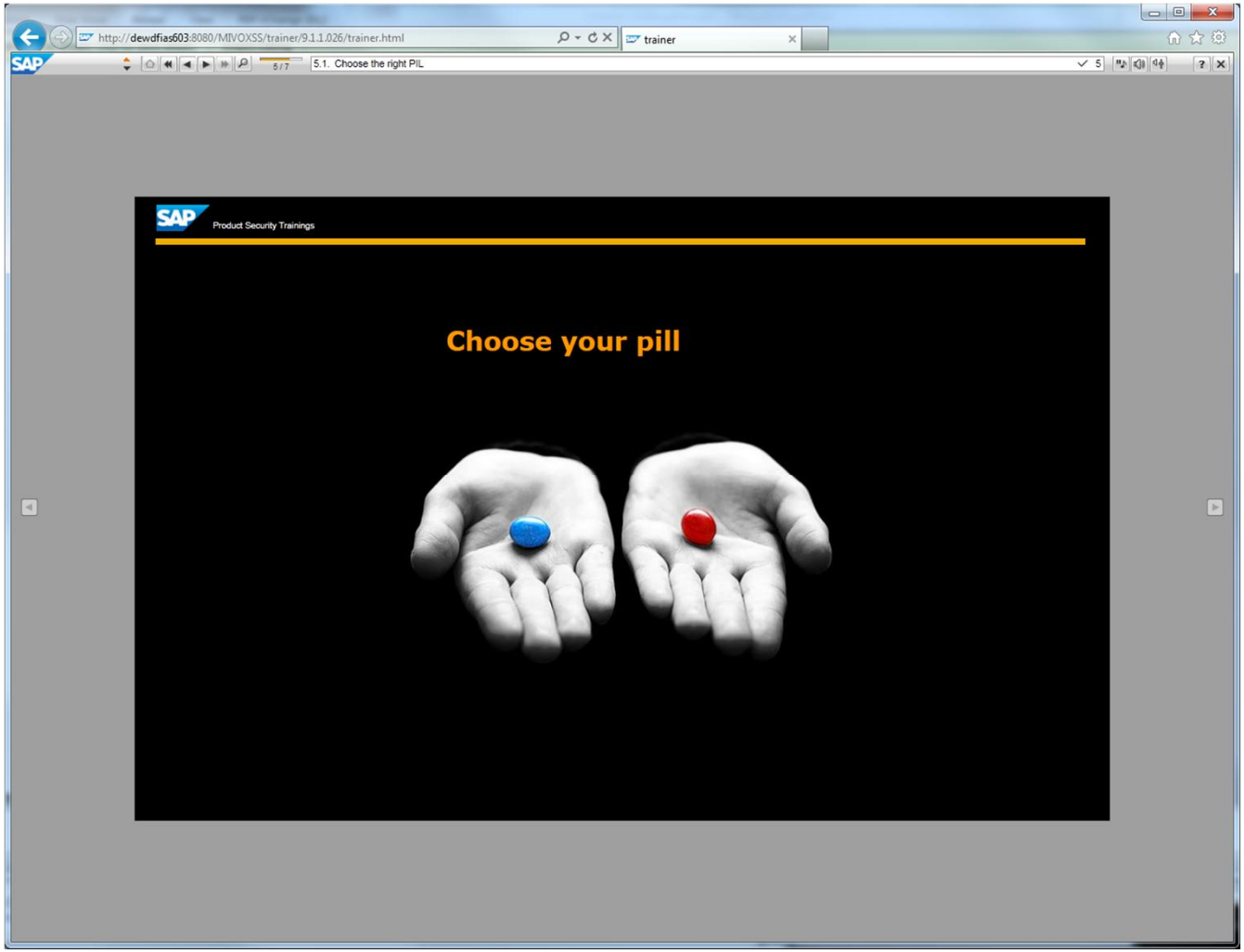
**Self-controlled**

**Entertaining**

**Rewarding**

**→ Gamification**

# Leave the Choice



# Definition

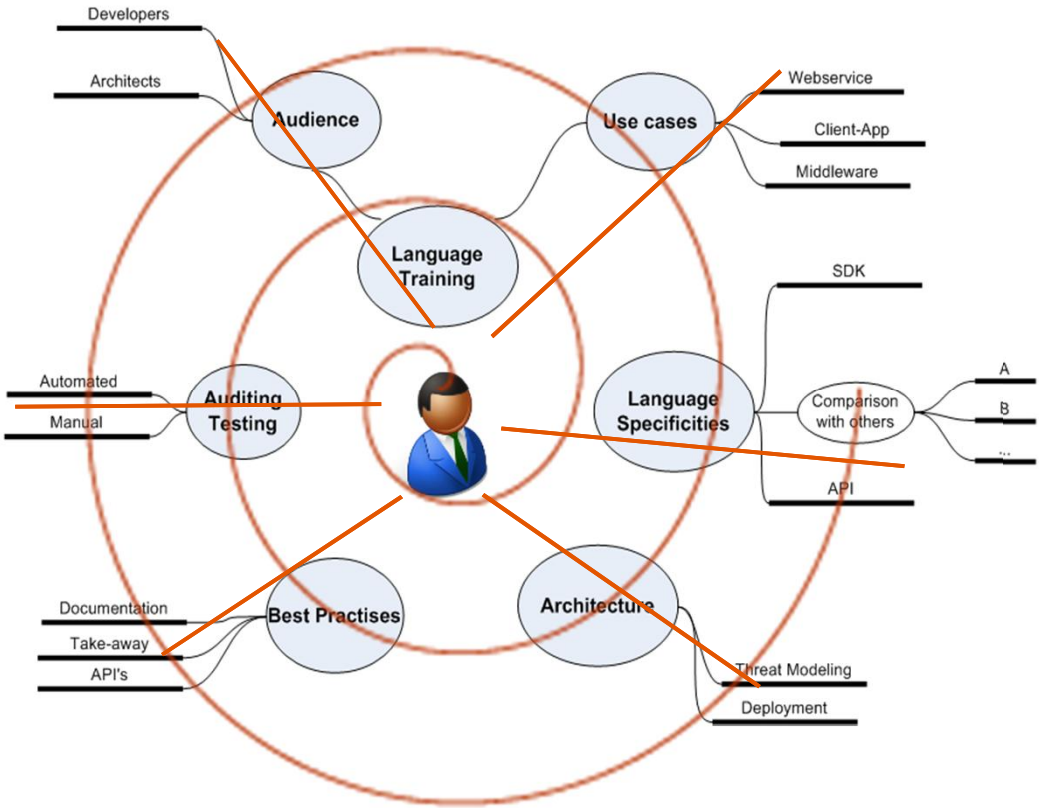
## Enterprise Gamification & Serious Gaming

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

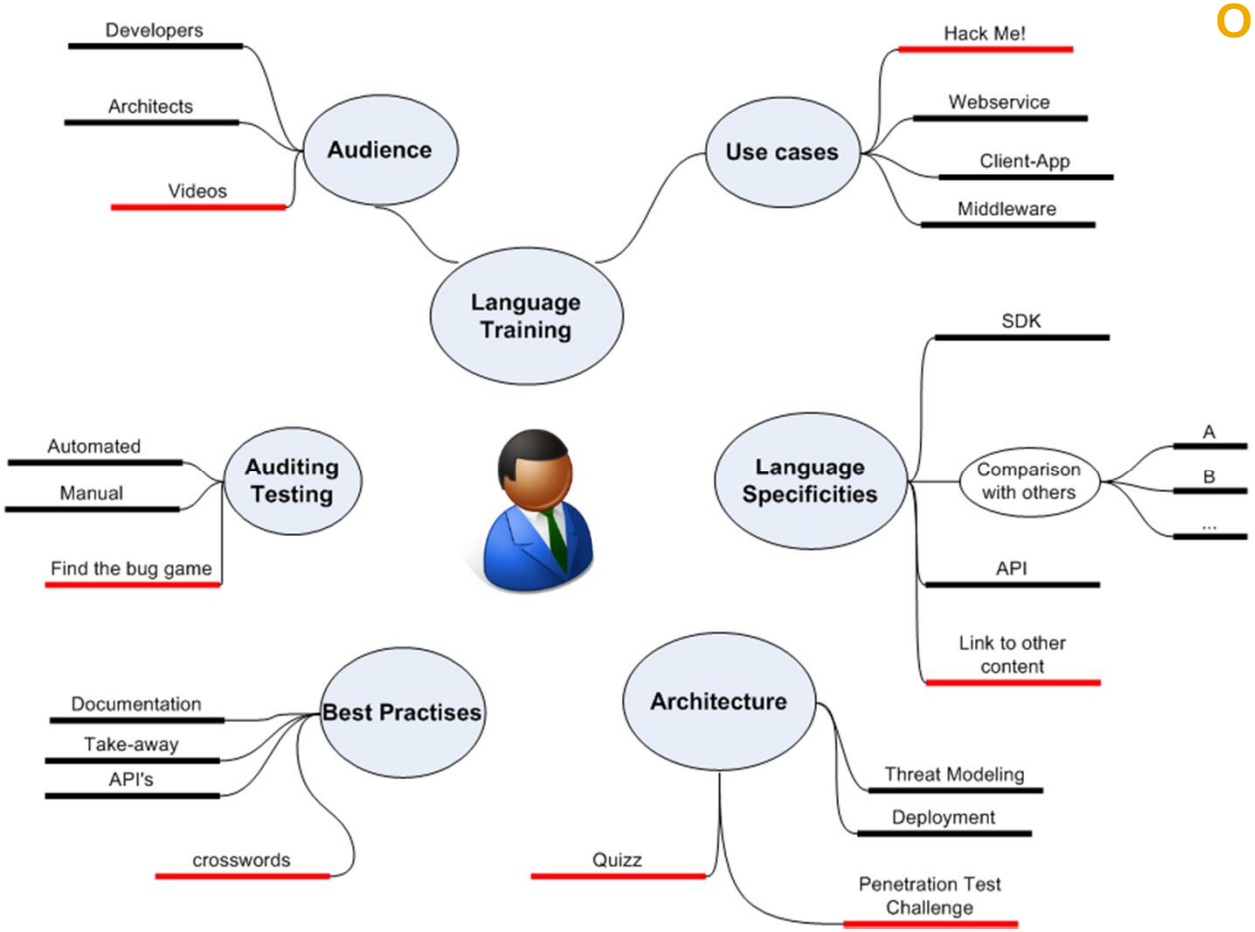



- micro-learning
  - Small units (15mn)
  - Self contained

# Example: Micro-learning

# Gamification in 3 steps: 2nd raise the excitement

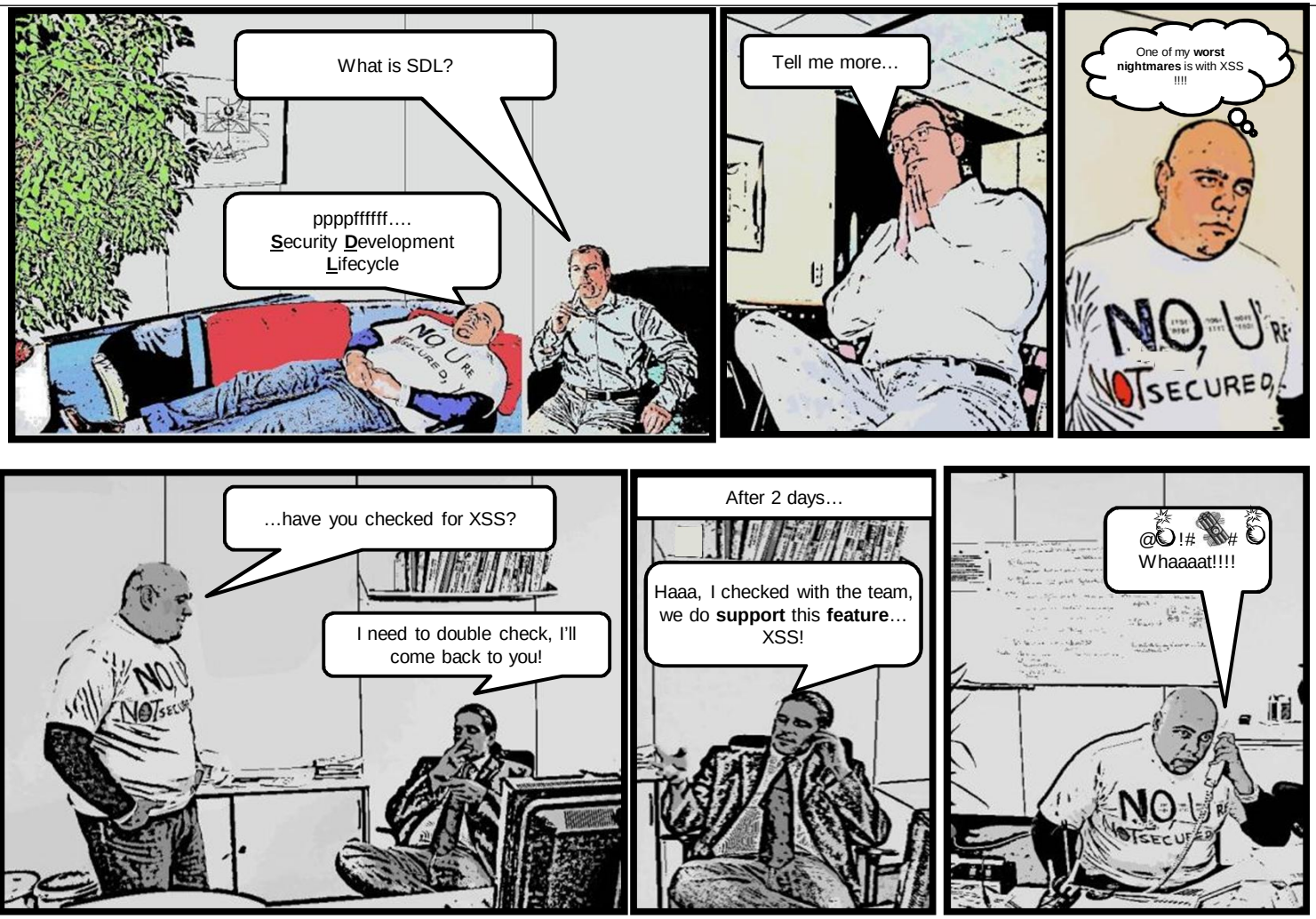
Interactivity and gamification on the content: making the content more attractive



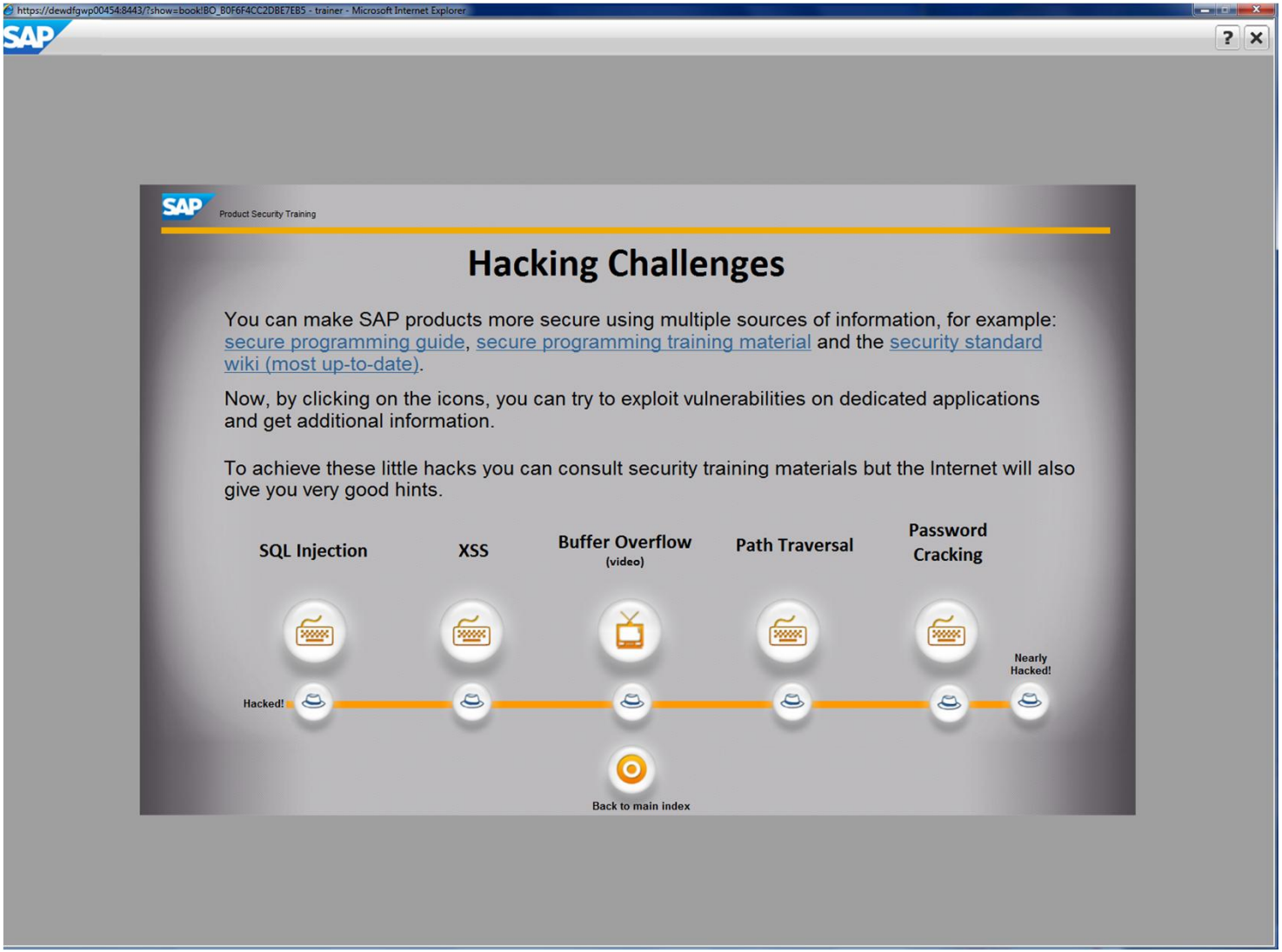

**Optional** content

- Static or interactive
- Challenging
- Entertaining

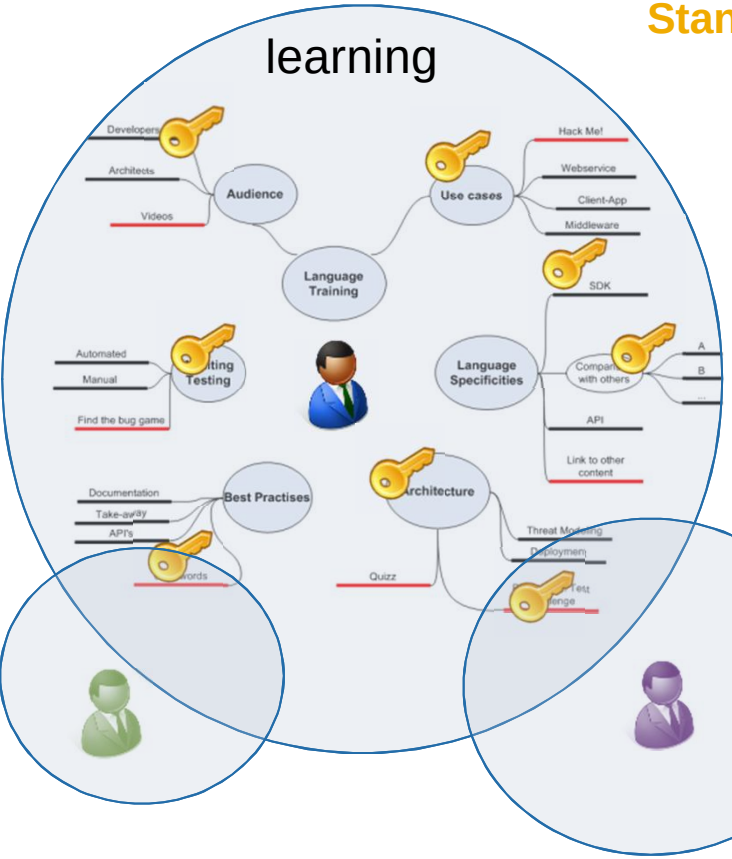
# Example: Storyboards



# Example: Challenges



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




**Standard** content

- progress bound to key acquisition (eg: via quizz)
- can be part of the game

**Optional** content

provide more keys

Hall of Fame

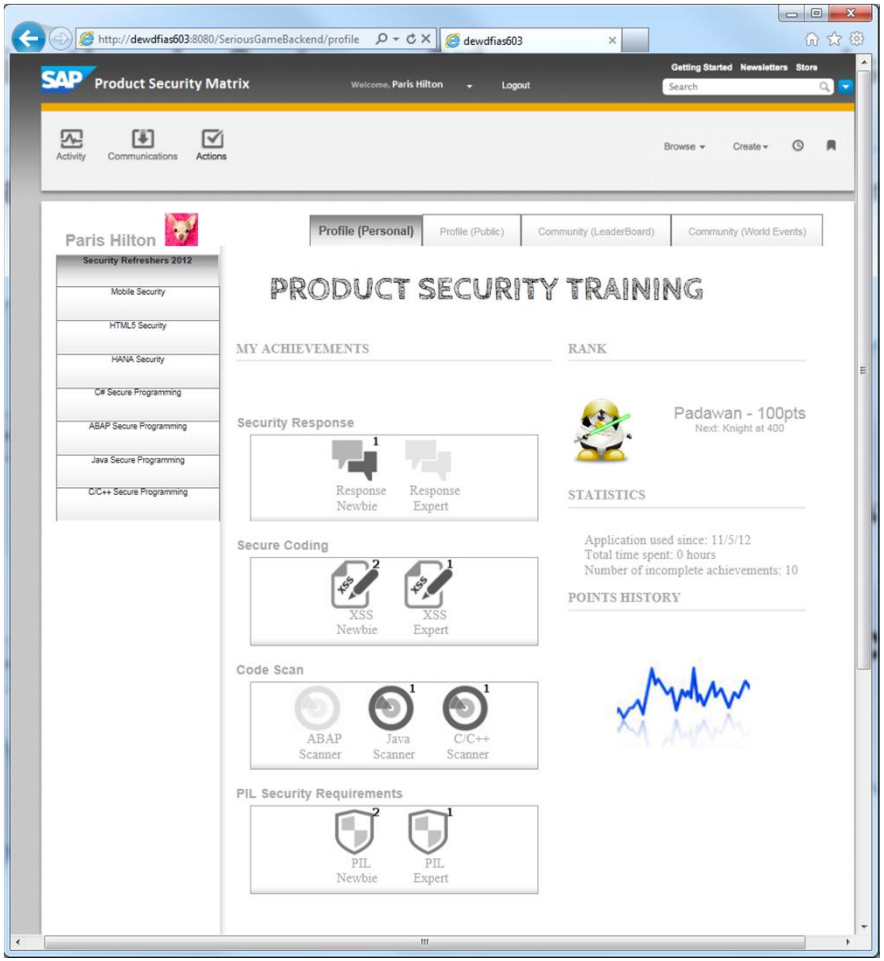
Awards

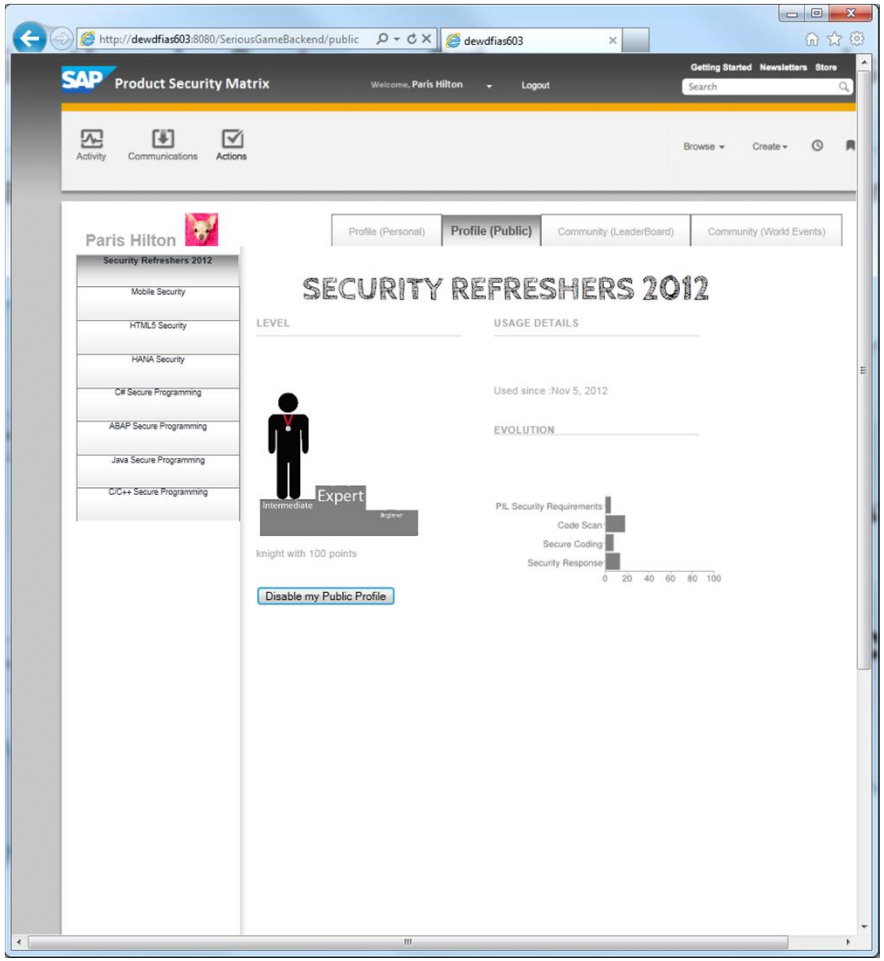
Competition

Communities

Contest

# Example: Achievements



# Take the Opportunity of Events

# 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!