

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

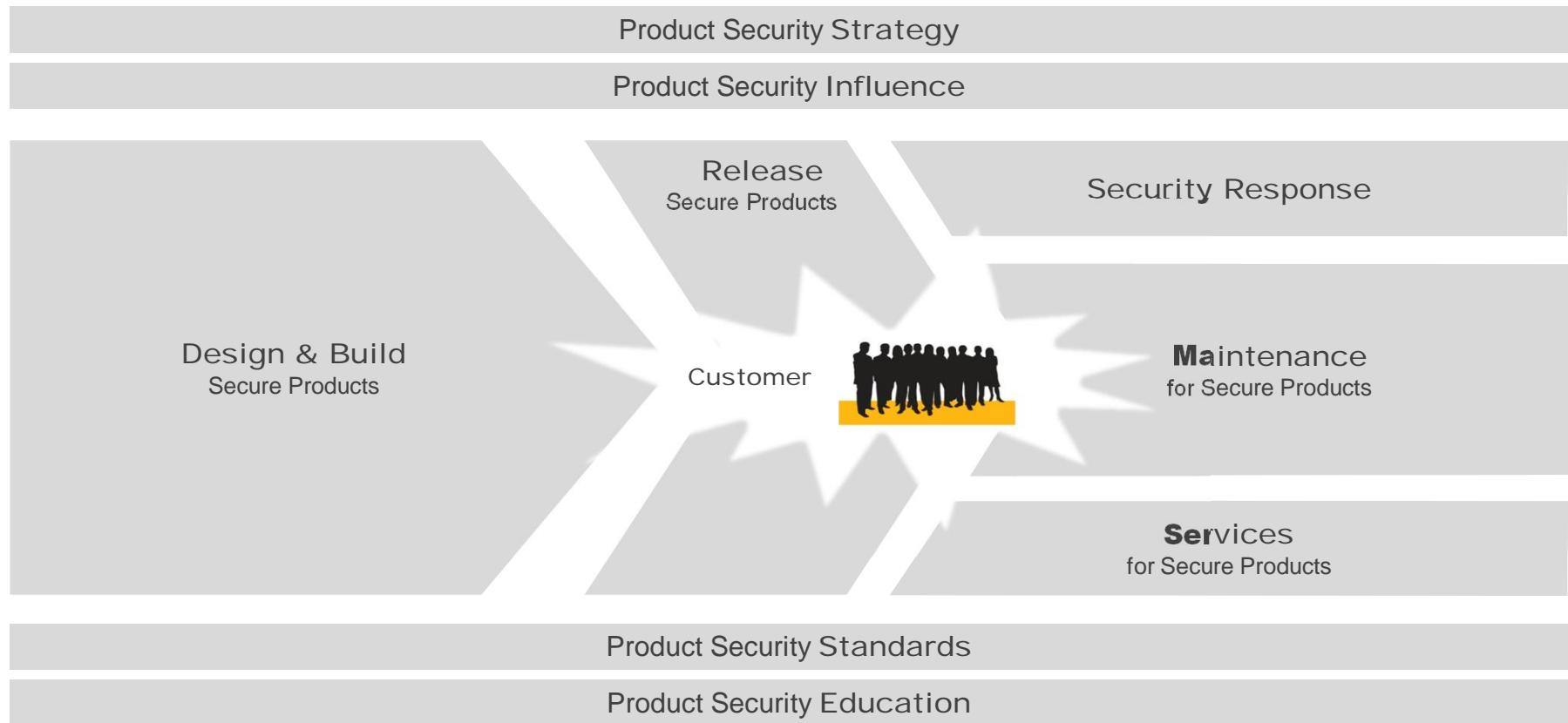
Part II – Retain Knowledge: Refresh & Extend

- 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

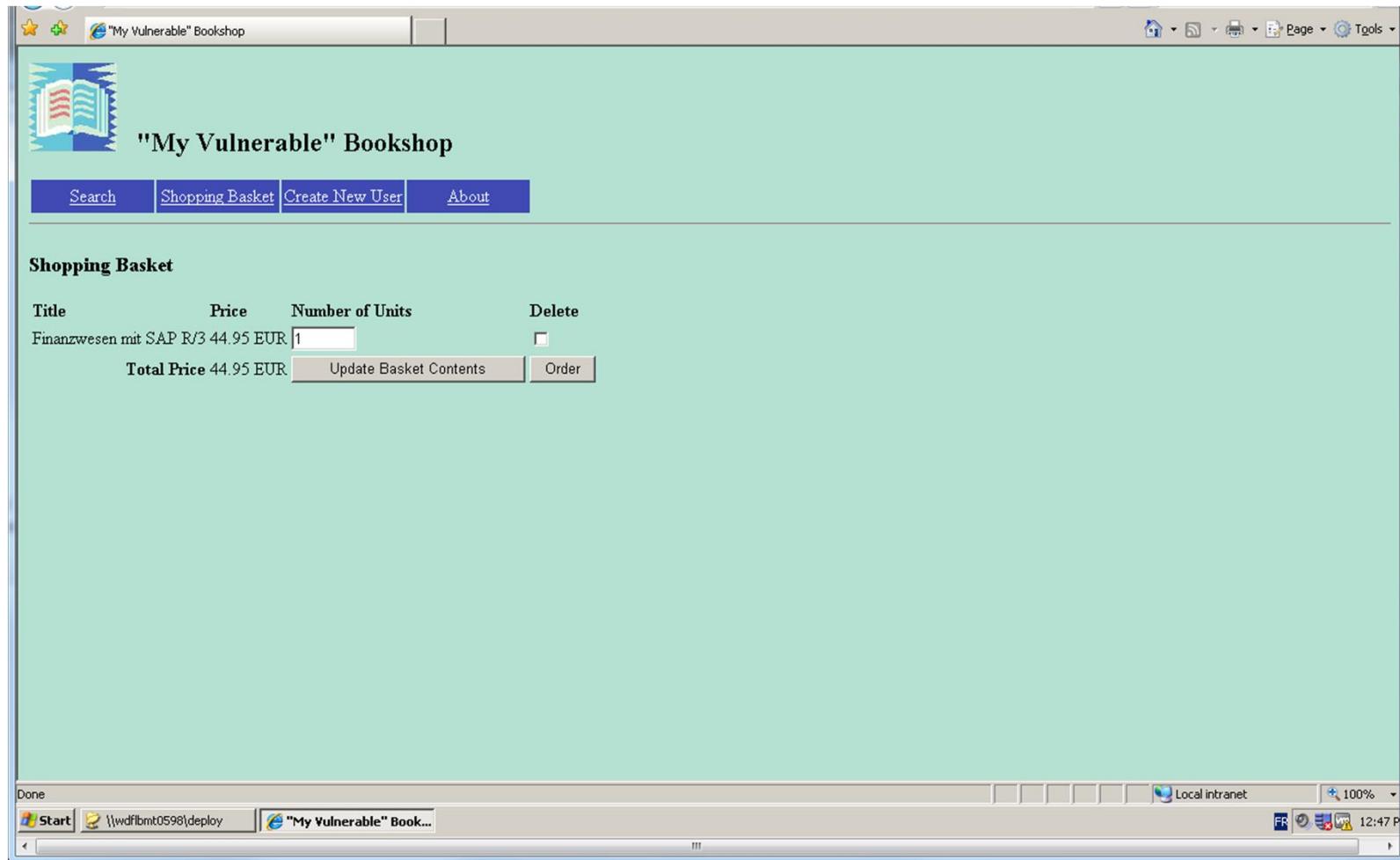
eLearning (1-day training only)

Community

Web Assessment

Exercises in Lab Environment

Example Exercise (1): My Vulnerable Bookshop



Example Exercise (2): XSS

cb-sac-nw701-demo - Remote Desktop Connection

Secure Programming (classroom group 00) - Microsoft Internet Explorer provided by SAP-Hosting

http://wdflbmt0598.wdf.sap.corp:8000/sap(bD1lbizjPTEwMA==)/bc/bsp/sap/z_stc_demo/XSS.htm

My Vulnerable Bookshop | Secure Programming (cla...)

Cross-site Scripting (XSS)

CWE-79 SEC-133

Startpage > Cross Site Scripting > Challenge

Challenge

In this challenge, your goal is to find a JavaScript code which opens a popup containing all cookies that you have received from this demo application. For that purpose you can exploit a XSS vulnerability being present in this small application.

Why searching for cookies? Among storing other things, cookies often contain authentication information and session identifiers. This information is very sensitive, and if attackers get hold of them, they can hijack your authenticated session without knowing your credentials (e.g., username and password), e.g., they can access your banking web page without the need to logon. The challenge is supposed to teach you how easy it is to access this information with JavaScript.

The initial purpose of the application is to simply print the provided string to the output page.

You find here three hints to support you in this challenge. In order to solve it, you have to enter the JavaScript snippet here.

Vulnerable application

EnterString:

Hints

Show/hide Hint #1

Simply enter JavaScript code into the input field.

Show/hide Hint #2

Answer the challenge

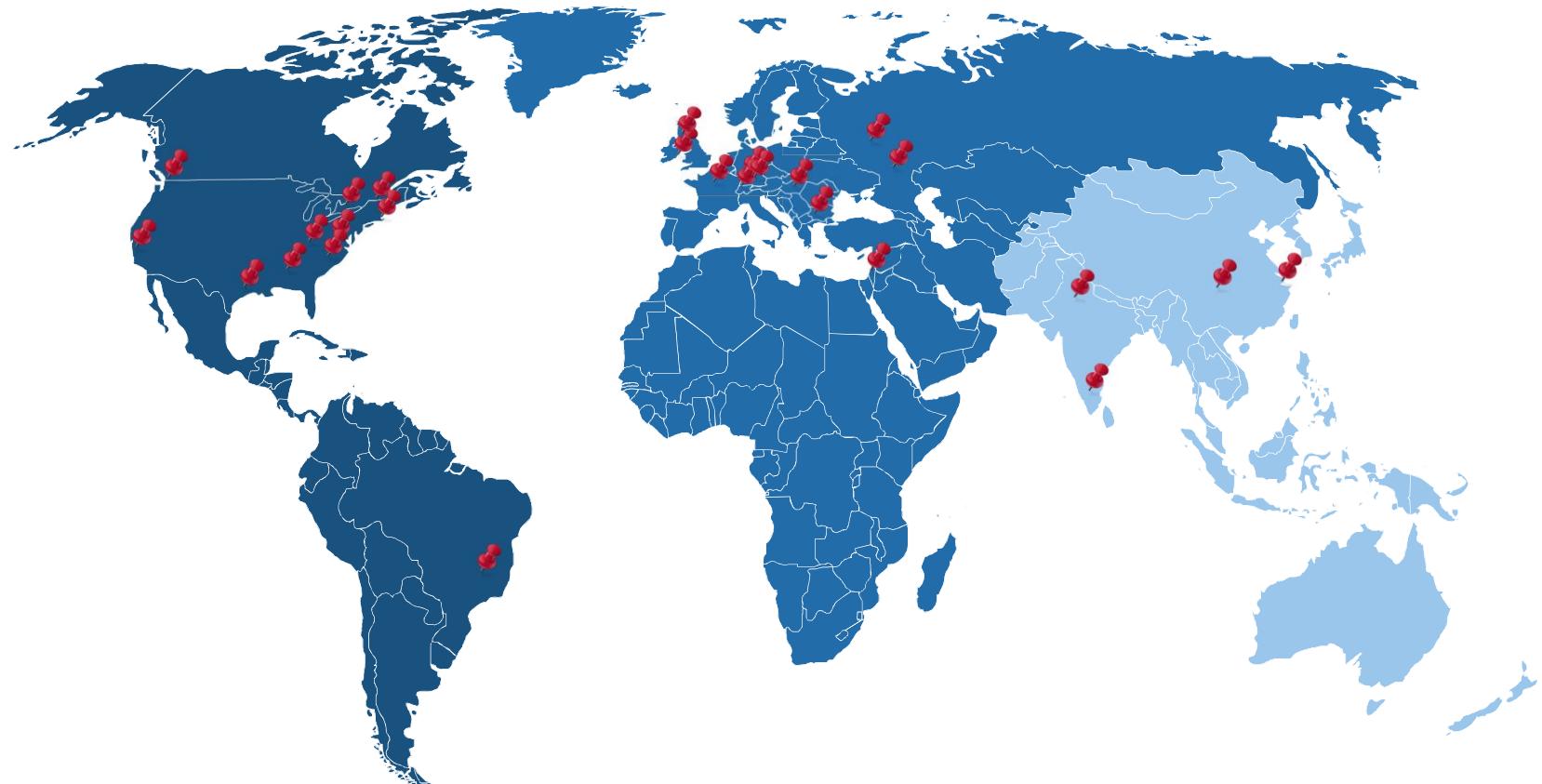
JavaScript snippet to display the cookie of the current session:

Local intranet 90% 12:49 PM

Start \wdflbmt0598\deploy Secure Programming ...

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

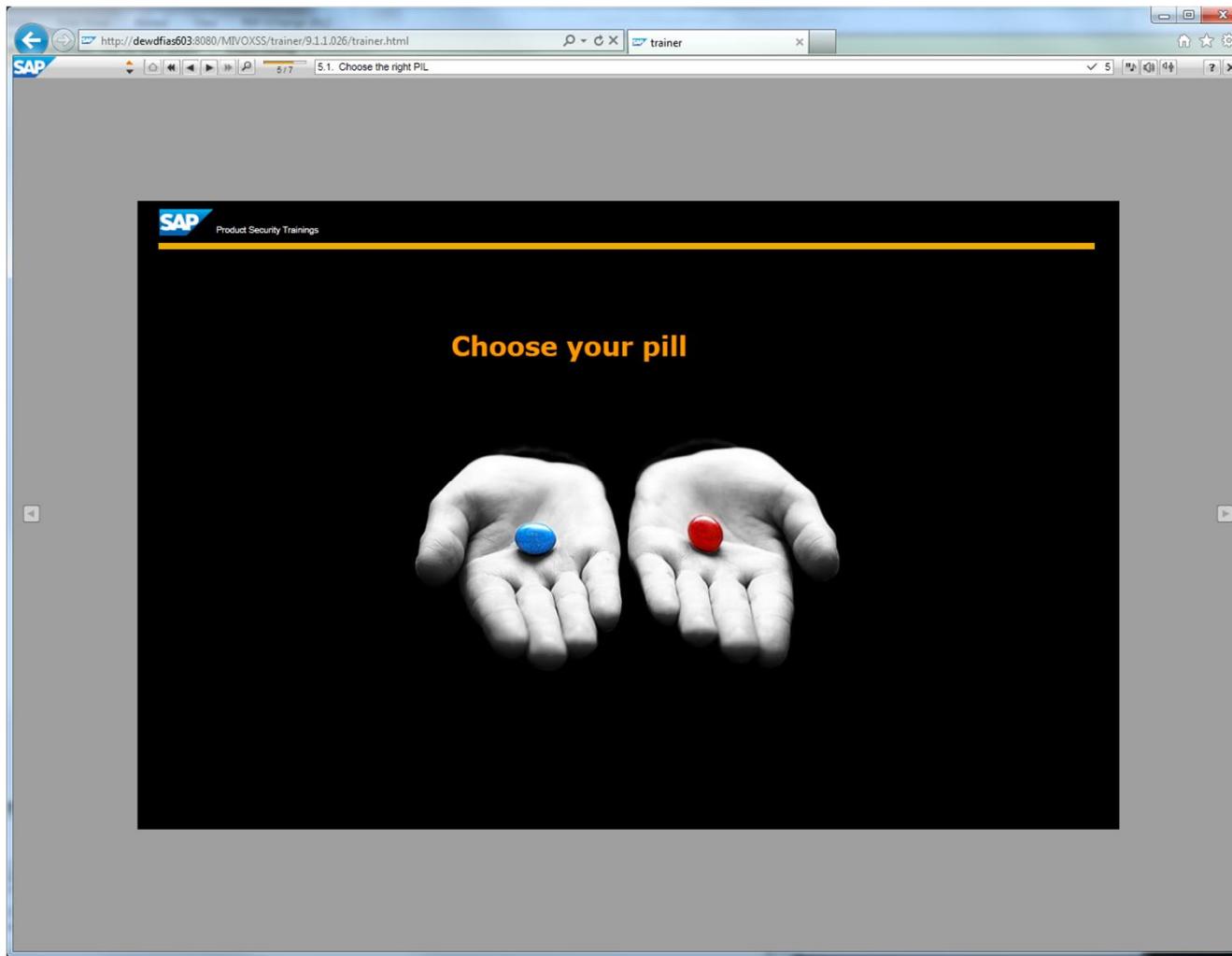
Self-controlled

Entertaining

Rewarding

→ **Gamification**

Leave the Choice



Definition

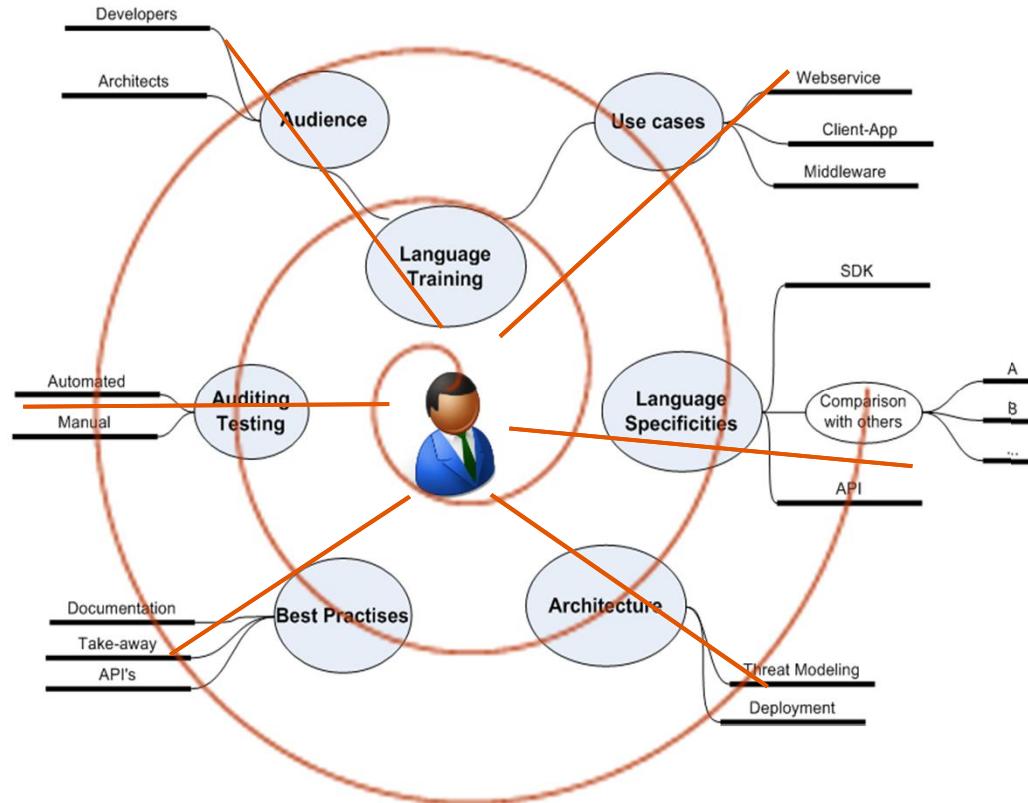
Enterprise Gamification & Serious Gaming

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

The screenshot shows a Microsoft Internet Explorer window displaying the SAP Product Security Training interface. The title bar reads "trainer - Microsoft Internet Explorer" and the address bar shows the URL: https://iwdfvm4897/wpb/wa/1/~tag/published/trainer/9.1.2.211/trainer.html?startMode=start&assignmentId=C_C4D8CF27FC554C0F8ED13B32AE81D77B&show=book!BO_722BC3FB4E256291.

The main content area features a central target icon with a blue center and orange concentric rings. The text "Leave the training" with a close button is in the top right. The interface is divided into four quadrants by a horizontal and vertical line:

- Product Standard Security** (top-left): Contains a brain icon.
- Secure Programming** (top-right): Contains a code editor icon.
- Product Security Response** (bottom-left): Contains a brain icon.
- Product Security Code Scans** (bottom-right): Contains a brain icon.

Each quadrant has a large orange question mark icon in its center. The entire interface is set against a light gray background.

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

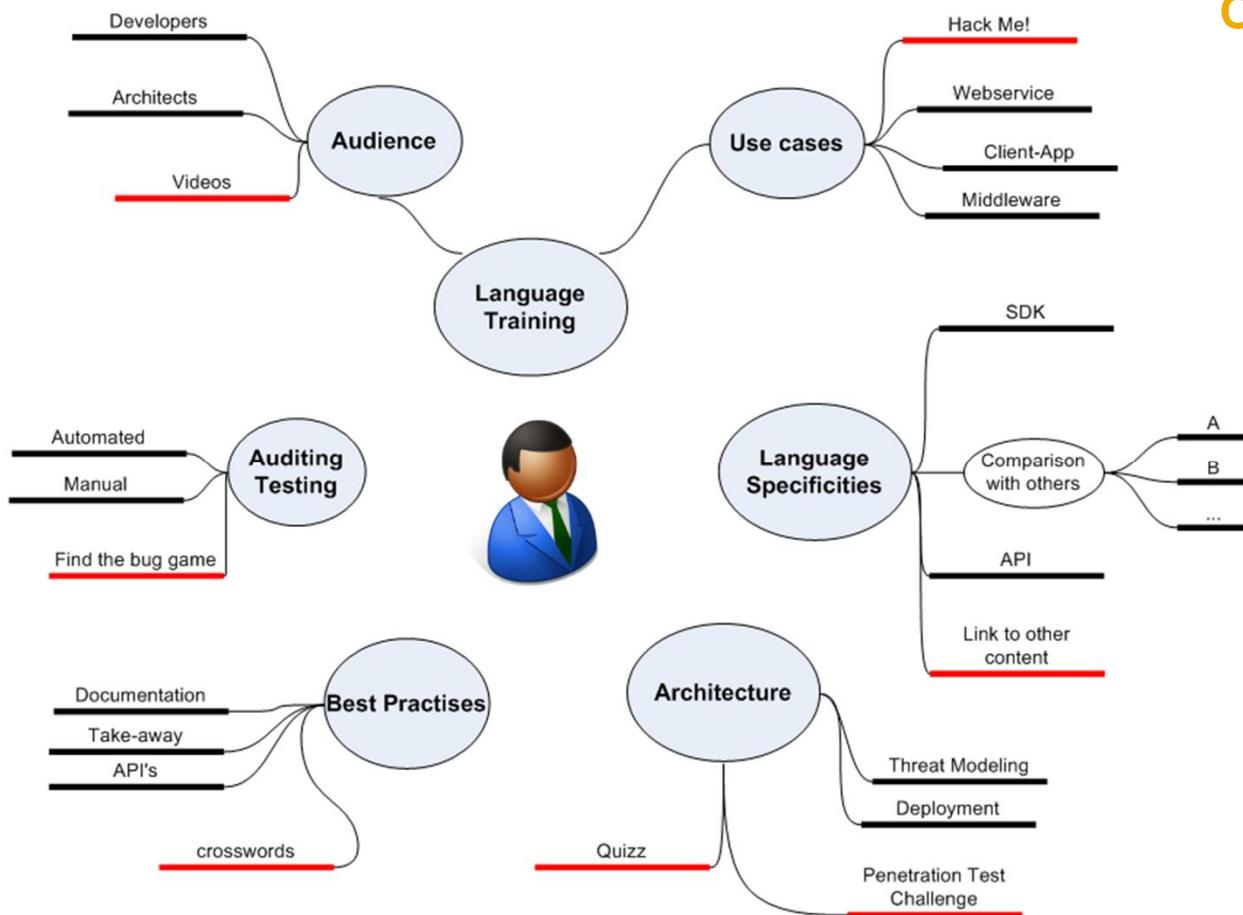
- Knowledge units are "must know"
- Practice units are "nice to know"
- Quizzes as another way to learn are "nice to know"
- Final unit to achieve the training

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



The screenshot shows a Microsoft Internet Explorer window displaying the SAP Product Security Training 'Hacking Challenges' page. The URL in the address bar is https://dewdfgwp00454:8443/?show=book!BO_B0F6F4CC2D8E7EB5-trainer. The page title is 'Hacking Challenges'. The content includes a paragraph about making SAP products more secure using multiple sources of information, followed by a list of five hacking challenges: SQL Injection, XSS, Buffer Overflow (video), Path Traversal, and Password Cracking. Each challenge is represented by a circular icon with a keyboard and a hat. A horizontal orange line connects the icons, with the first icon labeled 'Hacked!' and the last one labeled 'Nearly Hacked!'. A 'Back to main index' link is at the bottom.

https://dewdfgwp00454:8443/?show=book!BO_B0F6F4CC2D8E7EB5 - 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.

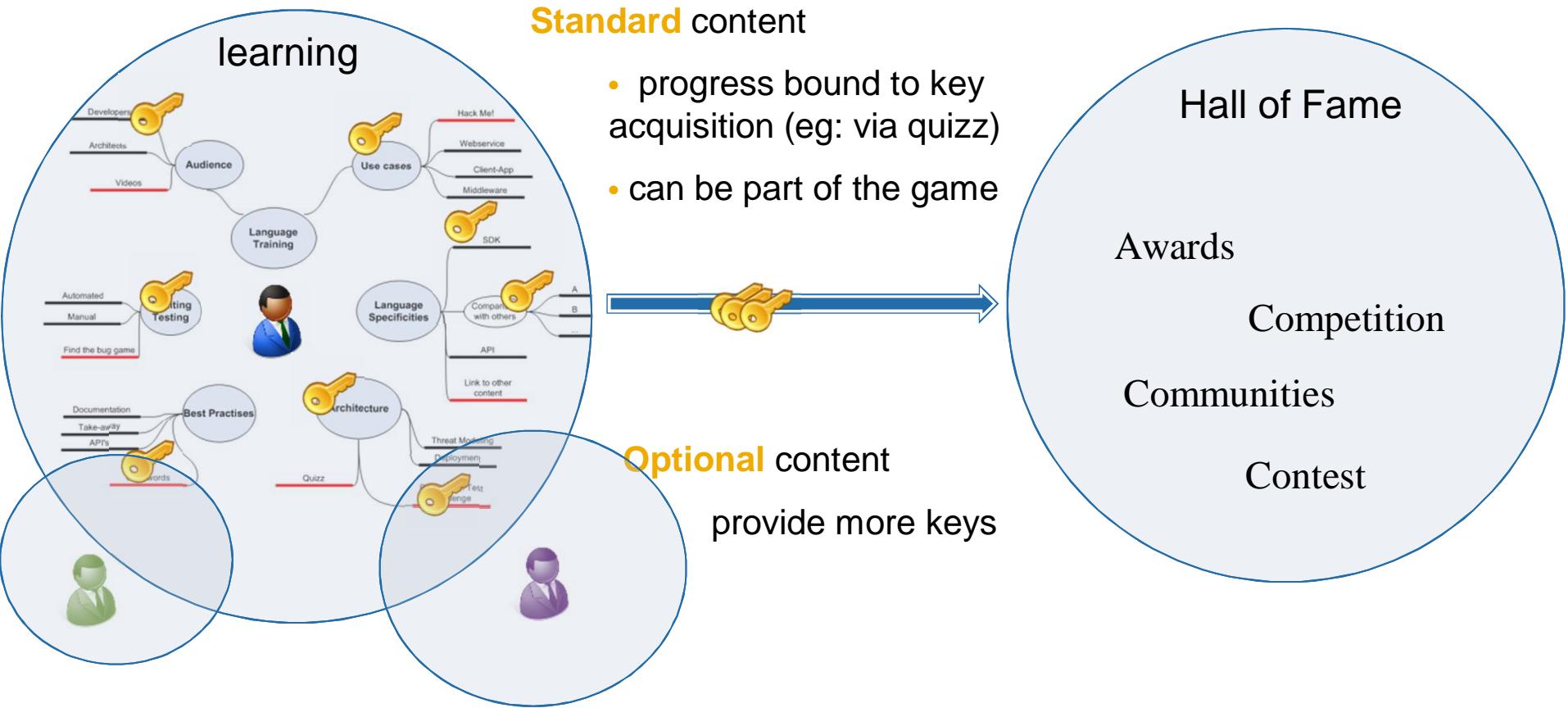
To achieve these little hacks you can consult security training materials but the Internet will also give you very good hints.

SQL Injection **XSS** **Buffer Overflow (video)** **Path Traversal** **Password Cracking**

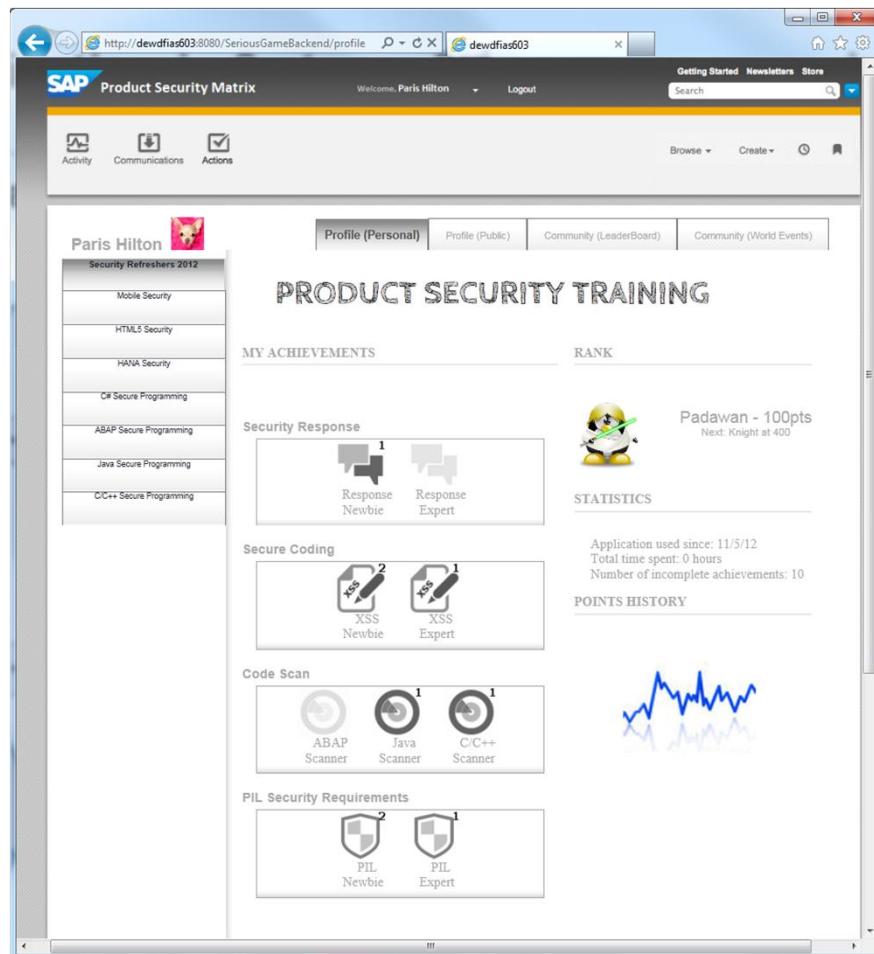
Hacked! Nearly Hacked!

Back to main index

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



Example: Achievements



SAP Product Security Matrix Welcome, Paris Hilton Logout

Profile (Personal) Profile (Public) Community (LeaderBoard) Community (World Events)

PRODUCT SECURITY TRAINING

MY ACHIEVEMENTS

- Security Response**
 - Response Newbie
 - Response Expert
- Secure Coding**
 - XSS Newbie
 - XSS Expert
- Code Scan**
 - ABAP Scanner
 - Java Scanner
 - C/C++ Scanner
- PIL Security Requirements**
 - PIL Newbie
 - PIL Expert

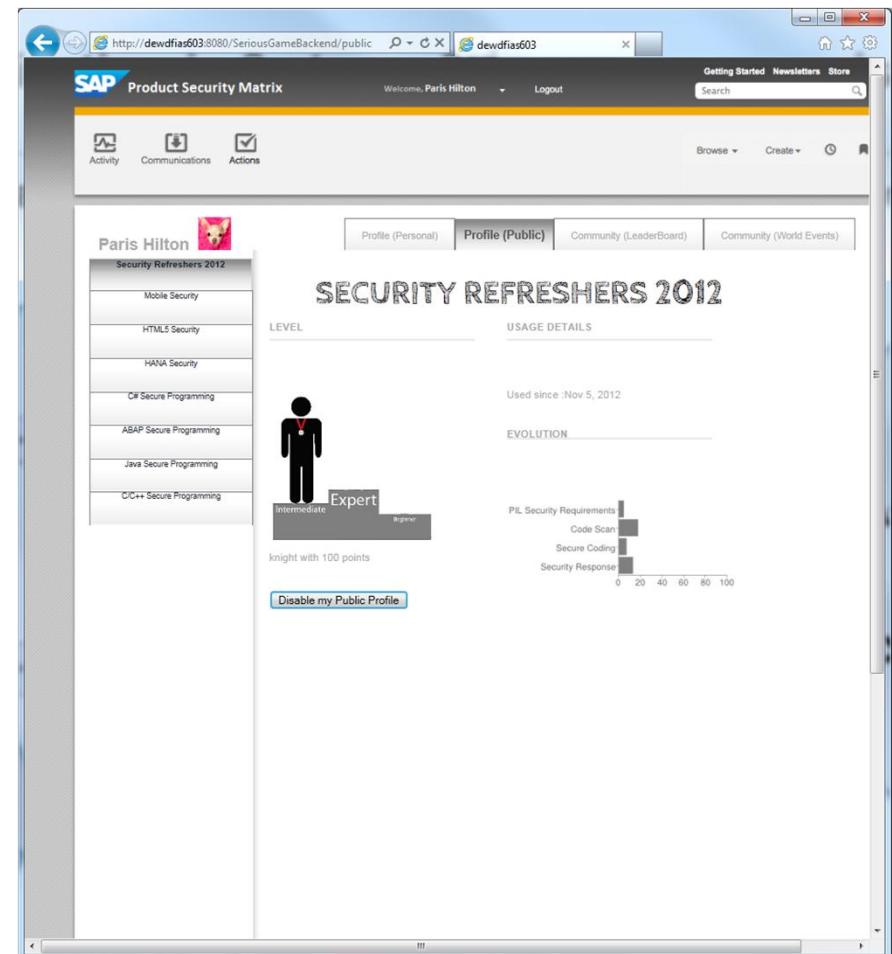
RANK

Padawan - 100pts
Next: Knight at 400

STATISTICS

Application used since: 11/5/12
Total time spent: 0 hours
Number of incomplete achievements: 10

POINTS HISTORY



SAP Product Security Matrix Welcome, Paris Hilton Logout

Profile (Personal) **Profile (Public)** Community (LeaderBoard) Community (World Events)

SECURITY REFRESHERS 2012

LEVEL

Used since: Nov 5, 2012

EVOLUTION

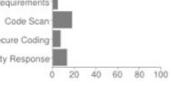
knights with 100 points

USAGE DETAILS

PIL Security Requirements

Code Scan	Secure Coding	Security Response
-----------	---------------	-------------------

Disable my Public Profile



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!