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

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Influence</th>
<th>Design &amp; Build</th>
<th>Release</th>
<th>Security Response</th>
<th>Maintenance</th>
<th>Services</th>
<th>Education</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Security</td>
<td></td>
<td>Secure Products</td>
<td>Secure Products</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td></td>
<td></td>
<td></td>
<td>Customer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2011 SAP AG. All rights reserved.
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
- Security Experts in Development Groups
- Solution Managers & Product Owners
- Managers & Development Project Managers
- Information Developers/ Technical Writers
- (Security) Testers
- Quality Managers

3 day Secure Programming

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

<table>
<thead>
<tr>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
</tr>
</thead>
</table>
| 9:00 – 10:00  
- Introduction | 9:00 – 10:30  
- Secure Programming  
Break | 9:00 – 10:30  
- Identity and Access Management  
Break |
| 10:00 – 11:00  
- Secure Programming  
Break | 11:00 – 12:00  
- Secure Programming  
Lunch | 11:00 – 12:00  
- Identity and Access Management  
Lunch |
| 11:30 – 12:30  
- Secure Programming  
Lunch | 13:00 – 15:30  
- Security Testing  
Break | 13:00 – 14:00  
- Security response |
| 13:30 – 15:00  
- Secure Programming  
Break | 16:00 – 17:00  
- Identity and Access Management | |
Training Formats

Classroom
Virtual Classroom
eLearning (1-day training only)
Web Assessment

Exercises in Lab Environment
Example Exercise (1): My Vulnerable Bookshop
Example Exercise (2): XSS

Cross-site Scripting (XSS)

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? Amongst 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 login. 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

Enter string: [ ]
Submit

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: [ ]
Submit
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: 1\textsuperscript{st} your need, your training

Personal Learning Environment: participant’s choice

- micro-learning
  - Small units (15mn)
  - Self contained
Example: Micro-learning
Gamification in 3 steps: 2\textsuperscript{nd} raise the excitement

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

**Optional** content
- Static or interactive
- Challenging
- Entertaining
Example: Storyboards

What is SDL?

ppppffffff.... Security Development Lifecycle

Tell me more...

...have you checked for XSS?

I need to double check, I'll come back to you!

After 2 days...

Haaa, I checked with the team, we do support this feature... XSS!

One of my worst nightmares is with XSS!!!
Example: 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.

<table>
<thead>
<tr>
<th>SQL Injection</th>
<th>XSS</th>
<th>Buffer Overflow (video)</th>
<th>Path Traversal</th>
<th>Password Cracking</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td><img src="image2.png" alt="Icon" /></td>
<td><img src="image3.png" alt="Icon" /></td>
<td><img src="image4.png" alt="Icon" /></td>
<td><img src="image5.png" alt="Icon" /></td>
</tr>
</tbody>
</table>

Hacked!

Back to main index
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

Product Security Summit

Android Challenge

We have located 231 People already

I made them a challenge they can not refuse!

I shouldn't tell that 34 blocked the Trojan
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!