Agenda

- Welcome / Petteri Arola, OWASP Helsinki Chapter Leader
- Word from our sponsor Helsingin Energia
- 3 different views on information security and social media applications
  - Information security in social media API’s, Antti Nuopponen/Nixu Oy
  - Facebook apps, Markus Törnqvist/Fad Consulting
  - Payment API’s, Tuomas Toivonen/Scred
OWASP Principles

- Free & Open

- Governed by rough consensus & running code

- Abide by a code of ethics:  

- Not-for-profit

- Not driven by commercial interests

- Risk based approach
OWASP Projects

- Quality Levels
  - Alpha, Beta, Release

- Organizational Structure within Tools and Docs
  - PROTECT - These are tools and documents that can be used to guard against security-related design and implementation flaws.
  - DETECT - These are tools and documents that can be used to find security-related design and implementation flaws.
  - LIFE CYCLE - These are tools and documents that can be used to add security-related activities into the Software Development Life Cycle (SDLC).
OWASP Application Security Verification Standard (ASVS)

- OWASP’s 1st Standard
- Defines 4 Verification Levels
  - Level 1: Automated Verification
    - Level 1A: Dynamic Scan
    - Level 1B: Source Code Scan
  - Level 2: Manual Verification
    - Level 2A: Penetration Test
    - Level 2B: Code Review
  - Level 3: Design Verification
  - Level 4: Internal Verification
What Questions Does ASVS Answer?

- How can I compare verification efforts?

- What security features should be built into the required set of security controls?

- What are reasonable increases in coverage and level of rigor when verifying the security of a web application?

- How much trust can be placed in a web application?
OpenSAMM

- Evaluate an organization’s existing software security practices
- Build a balanced software security assurance program in well-defined iterations
- Demonstrate concrete improvements to a security assurance program
- Define and measure security-related activities throughout an organization
Software Assurance Maturity Model (SAMM)

- The 4 **Disciplines** are high-level categories for activities
  - Three security **Functions** under each Discipline are the specific silos for improvement within an organization
SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘silo’ for improvement
The three levels for Practice

- (0: Implicit starting point with the Practice unfulfilled)
- 1: Initial understanding and ad hoc provision of the Practice
- 2: Increase efficiency and/or effectiveness of the Practice
- 3: Comprehensive mastery of the Practice at scale

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>...more on page 42</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EG 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EG 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EG 3</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Objective**

- **EG 1**: Offer development staff access to resources around the topics of secure programming and deployment
- **EG 2**: Educate all personnel in the software life-cycle with role-specific guidance on secure development
- **EG 3**: Mandate comprehensive security training and certify personnel for baseline knowledge

**Activities**

- **EG 1**
  - A. Conduct technical security awareness training
  - B. Build and maintain technical guidelines
- **EG 2**
  - A. Conduct role-specific application security training
  - B. Utilize security coaches to enhance project teams
- **EG 3**
  - A. Create formal application security support portal
  - B. Establish role-based examination/certification
Per Level, SAMM defines...

- **Objective**
- **Activities**
- **Results**
- **Success Metrics**
- **Costs**
- **Personnel**
- **Related Levels**
Conducting assessments

- SAMM includes assessment worksheets for each Security Practice

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>✦ Have most developers been given high-level security awareness training?</td>
<td></td>
</tr>
<tr>
<td>✦ Does each project team have access to secure development best practices and guidance?</td>
<td></td>
</tr>
<tr>
<td>✦ Are most roles in the development process given role-specific training and guidance?</td>
<td></td>
</tr>
<tr>
<td>✦ Are most stakeholders able to pull in security coaches for use on projects?</td>
<td>EG 1</td>
</tr>
<tr>
<td>✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?</td>
<td>EG 2</td>
</tr>
<tr>
<td>✦ Are most people tested to ensure a baseline skill-set for secure development practices?</td>
<td>EG 3</td>
</tr>
</tbody>
</table>