SAMM 2.0 - Changing the Role of App. Security
Yan Kravchenko,
CISSP, CSSLP, CISA, CISM
yan.kravchenko@concordusa.com
yan.kravchenko@owasp.org
@yanfosec
Agenda

1. Evolution of Programming Languages
2. Evolution of Development Methodologies
3. Why OWASP SAMM?
4. OWASP SAMM 2.0 Overview
Application Security Challenges

• Software development experience is rare among information security professionals
• Application security programs focus too much on post deployment testing
• Evolving cloud technologies create new opportunities and risks
• Programs still focus too much on individual vulnerabilities
Evolution of Programming Languages

Why do we need so many?

<table>
<thead>
<tr>
<th>Language Rank</th>
<th>Types</th>
<th>Spectrum Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Python</td>
<td>☰</td>
<td>100.0</td>
</tr>
<tr>
<td>2. C++</td>
<td>☰</td>
<td>99.7</td>
</tr>
<tr>
<td>3. Java</td>
<td>☰</td>
<td>97.5</td>
</tr>
<tr>
<td>4. C</td>
<td>☰</td>
<td>96.7</td>
</tr>
<tr>
<td>5. C#</td>
<td>☰</td>
<td>96.4</td>
</tr>
<tr>
<td>6. PHP</td>
<td>☰</td>
<td>94.9</td>
</tr>
<tr>
<td>7. R</td>
<td>☰</td>
<td>82.9</td>
</tr>
<tr>
<td>8. JavaScript</td>
<td>☰</td>
<td>82.5</td>
</tr>
<tr>
<td>9. Go</td>
<td>☰</td>
<td>76.4</td>
</tr>
<tr>
<td>10. Assembly</td>
<td>☰</td>
<td>74.1</td>
</tr>
<tr>
<td>11. Matlab</td>
<td>☰</td>
<td>72.8</td>
</tr>
<tr>
<td>12. Scala</td>
<td>☰</td>
<td>72.1</td>
</tr>
<tr>
<td>13. Ruby</td>
<td>☰</td>
<td>71.4</td>
</tr>
<tr>
<td>14. HTML</td>
<td>☰</td>
<td>71.2</td>
</tr>
<tr>
<td>15. Arduino</td>
<td>☰</td>
<td>69.0</td>
</tr>
<tr>
<td>16. Shell</td>
<td>☰</td>
<td>66.1</td>
</tr>
<tr>
<td>17. Perl</td>
<td>☰</td>
<td>57.4</td>
</tr>
<tr>
<td>18. Swift</td>
<td>☰</td>
<td>53.9</td>
</tr>
<tr>
<td>19. Processing</td>
<td>☰</td>
<td>53.1</td>
</tr>
<tr>
<td>20. Objective-C</td>
<td>☰</td>
<td>50.5</td>
</tr>
</tbody>
</table>
What’s your favorite text editor?

Go ahead... shout them out...
There are over 120...
Over 730 Programming Languages!!!
Interpreted vs. Compiled Languages

**Compiled**
- Hard to learn
- Requires Training
- Faster
- Stand-alone
- Commercial dependencies

**Interpreted**
- Easy to learn
- Amateur Friendly
- Slower
- Dependencies
- Open-Source dependencies
Interpreted Language Modules

- Subject to Open-Source Licensing
- Developed by enterprises, professional developers, and amateurs
- Software Supply-Chain is a new Threat Vector
## How Many Modules Do We Need?

<table>
<thead>
<tr>
<th>Repository</th>
<th>First Released</th>
<th>Total Count</th>
<th>Avg. Growth per Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPAN (Perl)</td>
<td>1987</td>
<td>39,908</td>
<td>3</td>
</tr>
<tr>
<td>PyPI (Python)</td>
<td>1991</td>
<td>179,176</td>
<td>131</td>
</tr>
<tr>
<td>Rubygems (Ruby)</td>
<td>1995</td>
<td>152,473</td>
<td>27</td>
</tr>
<tr>
<td>Maven Central (Java)</td>
<td>1995</td>
<td>280,028</td>
<td>124</td>
</tr>
<tr>
<td>Npm (node.js)</td>
<td>2009</td>
<td>818,768</td>
<td>560</td>
</tr>
</tbody>
</table>

Evolution of Computing Architecture
Evolution of Methodologies
Waterfall

- Requirements
- Analysis / Design
- Implementation
- Testing / Verification
- Deployment / Maintenance
Agile

Diagram: Idea → Design → Code → Test → Deploy
DevOps
How Different Are They?

Waterfall

Agile

DevOps
What is OWASP SAMM?

https://owaspsamm.org
A Little OWASP SAMM History

- **2009**
  - OpenSAMM 1.0
  - Funded by Fortify Security

- **2016**
  - OWASP SAMM 1.1
  - Added implementation guides

- **2017**
  - OWASP SAMM 1.5
  - Changed scoring model

- **2018–2019**
  - OWASP SAMM 2.0
  - The "DevOps Release"
OWASP SAMM 1.5 - Stable
Samm 2.0 Structure

- Governance
- Design
- Implementation (New)
- Verification
- Operations
What is Shifting Left?

• Consider the actual workflow of a developer

• Studies by NIST and Ponemon Institute provide a clear ROI

• Better and more frequent testing improves quality of each release
SAMM 2.0 - Governance

Governance

Strategy & Metrics
- Create and Promote
- Measure and Improve

Policy & Compliance
- Policy and Standards
- Compliance Management

Education & Guidance
- Training and Awareness
- Organization and Culture
SAMM 2.0 - Governance

- Start measuring something other than defect counts
- Re-write policies and compliance requirements as test scripts or runbooks
- Product Champions, not just Security Champions
SAMM 2.0 - Design

Design

Threat Assessment
- Application Risk Profile
- Threat Modeling

Security Requirements
- Software Requirements
- Supplier Security

Security Architecture
- Architecture Design
- Technology Management
SAMM 2.0 - Design

- Build granular application risk profiles
- Make requirements transparent and accessible
- Develop and document architectural standards
SAMM 2.0 - Implementation

Implementation

Secure Build
- Build Process
- Software Dependencies

Secure Deployment
- Deployment Process
- Secret Management

Defect Management
- Defect Tracking
- Metrics and Feedback / Learning
Make sure all application security team members can build a simple CI/CD Pipeline (https://www.owasp.org/index.php/OWASP_DevSecOps_Studio_Project)

Improve defect tracking analytics to identify trends
SAMM 2.0 - Verification

**Verification**

**Architecture Assessment**
- Architecture Validation
- Architecture Compliance

**Requirements Driven Testing**
- Control Verification
- Misuse / Abuse Testing

**Security Testing**
- Scalable Baseline
- Deep Understanding
SAMM 2.0 - Verification

Whenever possible, automate architecture checks.

Invest in tools to identify vulnerability as the code is written or committed.

Balance automated and manual penetration testing for the most effective and efficient results.
## SAMM 2.0 - Operations

### Operations

<table>
<thead>
<tr>
<th>Incident Management</th>
<th>Environment Management</th>
<th>Operational Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Incident Detection</td>
<td>• Configuration Hardening</td>
<td>• Data Protection</td>
</tr>
<tr>
<td>• Incident Response</td>
<td>• Patching and Updating</td>
<td>• System Decommissioning / Legacy Management</td>
</tr>
</tbody>
</table>


SAMM 2.0 - Operations

Plan for security incidents one application at a time

Configuration hardening and patching may look different, but are still necessary

Review test data routines
The DevOps Release...

• CI/CD pipeline publishes changes in minutes
  • https://owaspsamm.org

• Developed and maintained in Markdown
  • https://github.com/OWASP/samm/tree/master/v2.0/beta/core

• We want your feedback!
  • https://github.com/OWASP/samm/issues
Questions / Discussion

Thank you!