Welcome to the OWASP Toronto Meetup

Hello, and happy 2018!
Announcement: OWASP Top 10 2017
### Changes between 2013 and 2017

<table>
<thead>
<tr>
<th>OWASP Top 10 - 2013</th>
<th>OWASP Top 10 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - Injection</td>
<td>A1: 2017-Injection</td>
</tr>
<tr>
<td>A2 - Broken Authentication and Session Management</td>
<td>A2: 2017-Broken Authentication</td>
</tr>
<tr>
<td>A3 - Cross-Site Scripting (XSS)</td>
<td>A3: 2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A4 - Insecure Direct Object References [Merged+A7]</td>
<td>A4: 2017-XML External Entities (XXE) [NEW]</td>
</tr>
<tr>
<td>A5 - Security Misconfiguration</td>
<td>A5: 2017-Broken Access Control [Merged]</td>
</tr>
<tr>
<td>A6 - Sensitive Data Exposure</td>
<td>A6: 2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A8 - Cross-Site Request Forgery (CSRF)</td>
<td>A8: 2017-Insecure Deserialization [NEW, Community]</td>
</tr>
<tr>
<td>A9 - Using Components with Known Vulnerabilities</td>
<td>A9: 2017-Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10 - Unvalidated Redirects and Forwards</td>
<td>A10: 2017-Insufficient Logging&amp;Monitoring [NEW,Comm.]</td>
</tr>
</tbody>
</table>
Hi, I am X. How do I get into AppSec/Security?
Topics

- Overviews, Career Paths, Advice
- Secure SDLC frameworks
- Tools & Training
- Agile & DevSecOps
- Real Life Stories
- Training, Certifications and Career Fairs
Getting the Lay of the land

Find out what jobs/roles are commonly out there, figure out where your skills overlap, find out what skills you need, etc.

- NICE Cybersecurity Workforce Framework
- SANS CISO Mind Map (or, Reeq Rehman’s)
- Henry Jiang’s Map of Cyber Security Domains
- Cyberseek Career Pathway
Advice

Wisdom, editorials, and on-point snark

Krebs on Security - How to break into Security Series

(Older, but still relevant advice)
Secure SDLC: Some frameworks

- OWASP SAMM
- BSIMM
- DOE-C2M2
- NIST CSF
The Software Security Framework

The graphic below shows the software security framework (SSF) used to organize the 113 BSIMM activities. There are 12 practices organized into four domains.

The four domains are as follows:

- **Governance**: Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.
- **Intelligence**: Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.
- **SSDL Touchpoints**: Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.
- **Deployment**: Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

Here are the 12 practices:

**Governance**
1. Strategy & Metrics (SM)
2. Compliance & Policy (CP)
3. Training (T)

**Intelligence**
4. Attack Models (AM)
5. Security Features & Design (SFD)
6. Standards & Requirements (SR)

**SSDL Touchpoints**
7. Architecture Analysis (AA)
8. Code Review (CR)
9. Security Testing (ST)

**Deployment**
10. Penetration Testing (PT)
11. Software Environment (SE)
12. Configuration Management & Vulnerability Management (CMVM)

https://www.bsimm.com
## US Dept of Energy Capability Maturity Model

<table>
<thead>
<tr>
<th>Level</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIL0</td>
<td>Practices are not performed</td>
</tr>
<tr>
<td>MIL1</td>
<td>Initial practices are performed but may be ad hoc</td>
</tr>
</tbody>
</table>
| MIL2  | **Institutionalization characteristics:**  
          - Practices are documented  
          - Stakeholders are identified and involved  
          - Adequate resources are provided to support the process  
          - Standards or guidelines are used to guide practice implementation  
          **Approach characteristic:**  
          - Practices are more complete or advanced than at MIL1 |
| MIL3  | **Institutionalization characteristics:**  
          - Activities are guided by policy (or other directives) and governance  
          - Policies include compliance requirements for specified standards or guidelines  
          - Activities are periodically reviewed for conformance to policy  
          - Responsibility and authority for practices are assigned to personnel  
          - Personnel performing the practice have adequate skills and knowledge  
          **Approach characteristic:**  
          - Practices are more complete or advanced than at MIL2 |

### Domains
- **Risk Management**
- **Asset, Change, and Configuration Management**
- **Identity and Access Management**
- **Event and Incident Response, Continuity of Operations**
- **Supply Chain and External Dependencies Management**

- Domains are logical groupings of cybersecurity practices
- Each domain has a short name for easy reference
## NIST Cyber Security Framework

<table>
<thead>
<tr>
<th></th>
<th>Asset management</th>
<th>Access control</th>
<th>Protective technology</th>
<th>Response planning</th>
<th>Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Business management</td>
<td>Awareness and training</td>
<td>Anomalies and events</td>
<td>Communications</td>
<td></td>
</tr>
</tbody>
</table>
General Sources of Info

Teach yourself, then keep up with the field.

Infosec industry site has some recommendations you can pick through.

Blogs like SANS AppSec Blog and Google Project Zero

Twitter #appsec and major players, including Michael Geist and Office of the Privacy Commissioner of Canada

Security Podcasts like Defensive Security
Alternatives to YouTube, which actually has some pretty neat stuff on it too.

- Coursera
- Cybrary
- edX
- Lynda (free via Library!)
- MIT Open Courseware
- Udacity
- Udemy
What is your job title, and what sources of information do you use regularly?
Point of View: Developers and Testers
OWASP resources

OWASP has a lot of projects that can be helpful for developers to start learning about security. Two good starting points:

- A Quick Developer’s Guide
- OWASP Security Knowledge Framework

https://create.piktochart.com/output/6400107-untitled-infographic
Free Secure Coding Resources*

- OWASP Resources
  - OWASP Code Review Guide
  - OWASP Developer/Builder Cheat Sheets
- Secure Coding Exercises
  - Hacksplaining
  - Code Bashing
  - RIPSTECH PHP Security Advent Calendar
- Other Publications
  - CERT Secure Coding
  - Safecode training

* The latter resources also can be mined for other security-related info.
Security Testing Resources

Learn about the basic classes of application security vulnerabilities with hands-on, practical, guided lessons.

Deliberately Vulnerable Applications

- OWASP Juice Shop
- OWASP WebGoat
- OWASP Security Shepherd

HTTP Proxies (+ other awesomeness)

- OWASP Zed Attack Proxy (ZAP)
- Burp Suite Community Edition
- Kali Linux (+ forensics mode)
Capture the Flag!

Training Wheels are off.... Go hack stuff.

An Intro to CTFs

CTF Time Calendar

Vulnerable VMs to practice on in a lab, often abstracted from CTFs.

- https://www.vulnhub.com/ (they also suggest some resources)
Real Life Challenges

Legally try your skills against real targets.

Be sure to read the instructions, code of ethics, and bounty rules.

Whitehat CERN hacking challenge (students only)

Bug Bounty Programs
Agile?

- Secure SDLC vs CI (Continuous Integration) and CD (Continuous Development / Delivery / Deployment)
- **SDL-Agile Requirements**?
- Thoughts from the audience?
Point of View: Dev Ops
Secure DevOps Toolchain from SANS

https://www.sans.org/security-resources/posters/secure-devops-toolchain-swat-checklist/60/download
Additional DevSecOps Resources

Whether you stay earthbound or go to the cloud.

- OWASP Appsec Pipeline
- DevSecOps Studio
- Awesome DevSecOps
- AWS codepipeline devsecops
Point of View: Non-Devs
Learn to Program

Scripting experience and compiled language programming are both good to have.

Check out Laurence Bradford’s list of resources..

- [Free Code Camp](#)
- [Code Wars](#)
Security Origin Stories
Certifications & Career Fairs
(ISC)²

- Not free!
- CISSP (Certified Information Systems Security Professional)
  - Concentrations:
    - ISSAP (Architecture)
    - ISSEP (Engineering)
    - ISSMP (Manager)
- Relevant to application security:
  - CSSLP (Certified Secure Software Lifecycle Professional)
- Others:
  - CCSP (Cloud)
SANS Courses / GIAC Certifications

- Not free!
- SANS training courses with associated GIAC certifications
- Relevant to application security:
  - GWAPT
  - GWEB
  - GSSP-JAVA, GSSP-NET
Pen Testing Certifications

- Offensive Security Certified Professional (heavy focus on network-based content, but still somewhat relevant)
Product Specific Certifications

- CCNA / CCNE
- Security+
Career Fairs

- **Sheridan College Biztech**: February 14, 2018
- **SecTor Expo**: October 1-3, 2018
- **TASK**: TBD
Audience...

- AppSec / Security professionals:
What training or certifications or skills have you found to be most useful to your career?

- Hiring managers:
What do you like to see in candidates?
Questions? Closing Comments?