Teaching the OWASP Top 10 to Beginning Developers

Olivia Liddell
Technical Curriculum Developer,
Amazon Web Services

@oliravi

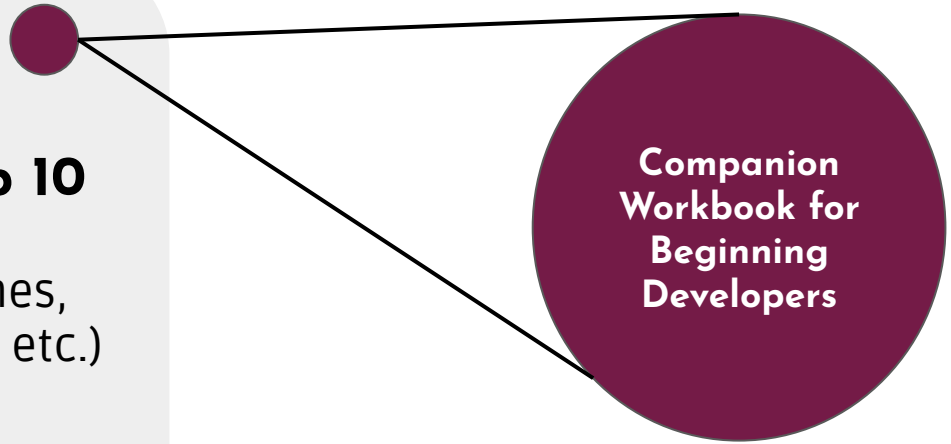
Where this idea began

Learning about application security doesn't have to look like this.

Where does this project fit in?

Teaching the OWASP Top 10

(All possible teaching approaches, learning tools, target audiences, etc.)

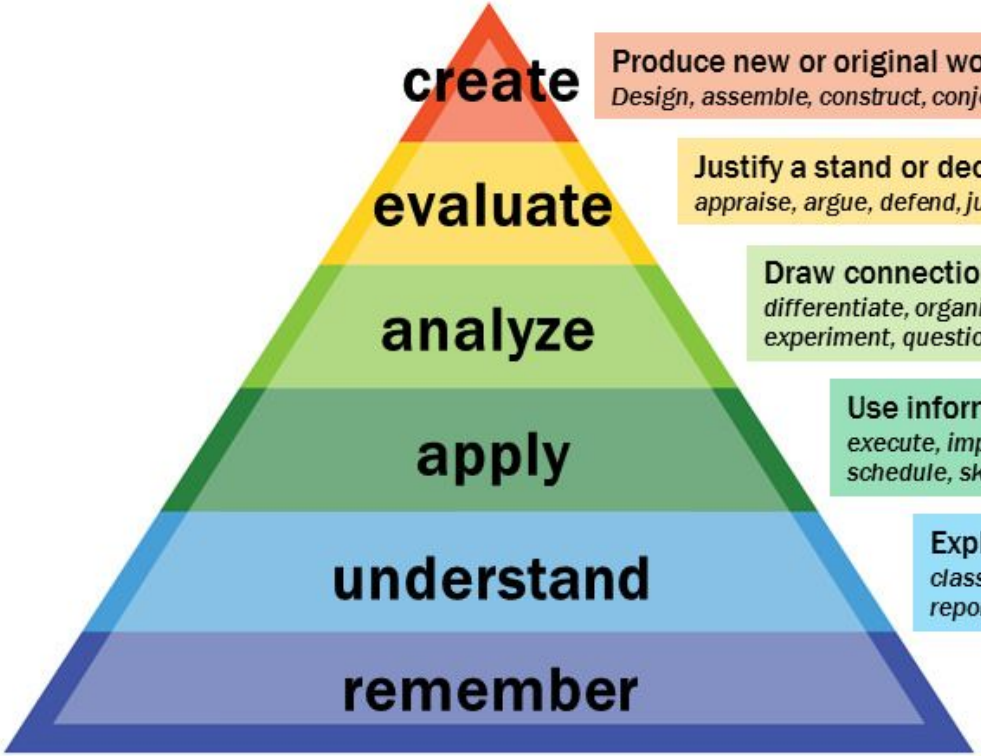


Working backwards: Guiding questions

- **Who** do I want to help?

- What should learners be able to **do** as a result of completing this workbook?

Bloom's Taxonomy



Produce new or original work
Design, assemble, construct, conjecture, develop, formulate, author, investigate

Justify a stand or decision
appraise, argue, defend, judge, select, support, value, critique, weigh

Draw connections among ideas
differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test

Use information in new situations
execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch

Explain ideas or concepts
classify, describe, discuss, explain, identify, locate, recognize, report, select, translate

Recall facts and basic concepts
define, duplicate, list, memorize, repeat, state

Working backwards: Guiding questions

- **Who** do I want to help?
  Beginning developers

- What should learners be able to **do** as a result of completing this workbook?
  - Identify the risks that are included in the OWASP Top 10.
  - Describe the Top 10 risks.
  - Compare and contrast risks.
  - Relate the Top 10 risks and prevention strategies to real-life scenarios.

Reordering the Top 10

Official OWASP Order

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

Order in the Companion Workbook

1. Using Components with Known Vulnerabilities (+8)
2. Security Misconfiguration (+4)
3. Broken Access Control (+2)
4. Insufficient Logging and Monitoring (+6)
5. Broken Authentication (-3)
6. Sensitive Data Exposure (-3)
7. Injection (-6)
8. Cross-Site Scripting (XSS) (-1)
9. Insecure Deserialization (-1)
10. XML External Entities (XXE) (-6)

Focus area #1: The *language* of security

"We cannot really teach language.

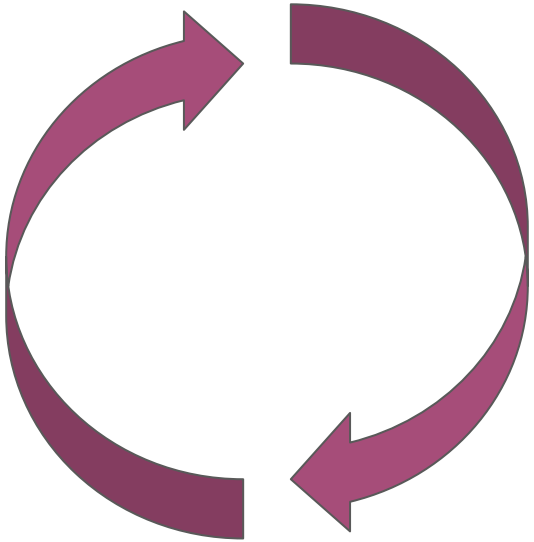
We can only create conditions in which it will develop spontaneously in the mind in its own way."

- **Wilhelm von Humboldt**
  (German linguist, 1767-1835)

Focus area #2: Reflection and metacognition

Reflection:

What do I know?



Metacognition:

How do I know that I know this?

These are two essential building blocks that can help to establish a solid foundation for beginners.

Sample section from the companion workbook

Broken Access Control

Access permissions are another aspect of application security. When you think about all of the users who have accounts within an application, imagine what might happen if every user had full administrator access. In this situation, users would most likely be able to access all parts of the application, make changes to application settings, and even modify other users' account information.

Broken access control occurs when users are able to access information and perform actions that are outside of their intended permissions.

How is broken access control similar to security misconfiguration? How does it differ?

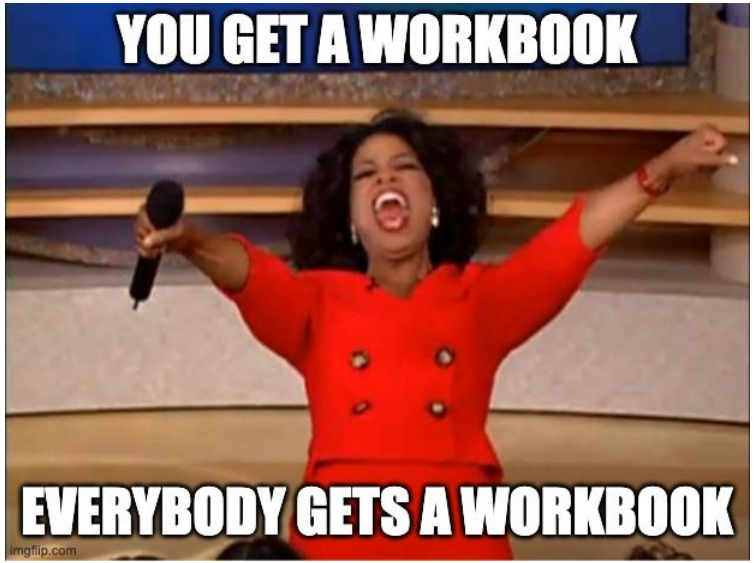
Pilot feedback

- Very well-designed for the target audience!
- The reflection exercises helped to spark insightful thoughts for learners.
- Determining the right amount of content to include for each risk
- Key point to include: Real-world trade-offs that often need to be made to balance security with a company's other priorities
- Consider including multiple-choice review questions for each risk.

Next steps

- Excited to see how more developers will respond to the workbook!

- Plan to incorporate this into a conference workshop that will include hands-on coding exercises, group discussions, etc.



Thank you!

olivialiddell.com