Security Champions

Only YOU Can Prevent File Forgery!

Marisa Fagan
at QCon London 2018

QCon
LONDON

Agenda

- Who am I?
- What’s a Security Champion?
- What can YOU do as the lone champion?
- What can your company do to support YOU?
- Takeaways

Who am I?

- Marisa Fagan: Life-long cool person
- Information Security Professional for 10 years
  - Building communities and spreading the hacker mindset
  - Studying Secure Development practices
- Product Security Lead at Synopsys

What is a Security Champion?

- An advocate for stronger code
- A Senior Developer or Engineer
  - Understands how changes affect the product
- Extra secure coding training
- Evangelist for security requirements
- Additional Security testing activities

How YOU can be the lone Champion?

- Start with extra security training
- Create a Threat Model
- Find defective low hanging fruit
- Share your discoveries with the team
- Ask the security team about cross-team collaboration

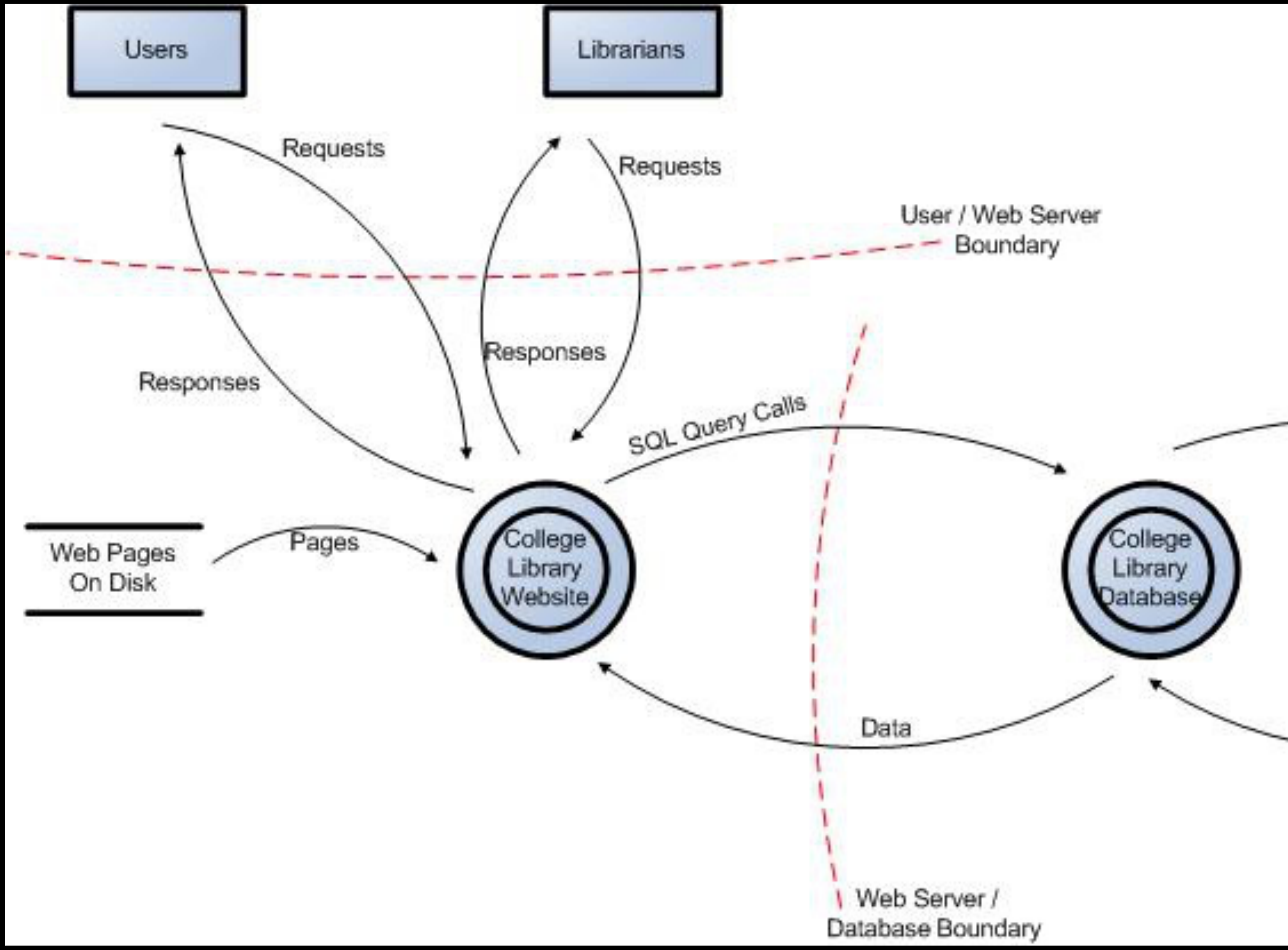
Training

- Secure Coding Training covers:
  - XSS, SQL Injection, RBAC, CSRF, Misused Direct Object Reference, Protecting Sensitive Data, Broken Auth & Session Mgmt, and Misconfigurations
  - Security testing tutorials for static analysis tools
  - Threat Modeling concepts

Be sure to check out presentation: Is Boilerplate Code Really So Bad? by Trisha Gee
Wednesday at 4:10pm in Mountbatten for more Java related secure code concepts

Threat Modeling

- Decompose the app to assets, entry points, and trust boundaries
- Threat analysis list (STRIDE) with risk model (DREAD)
- Threat Model SDK: A Java library for parsing and programmatically using threat models (stevespringett)



1. Start with a Data Flow Diagram

Be sure to stay for Presentation: Attack Trees, Security Modeling for Agile Teams by Michael Brunton-Spall at 5:25 Monday in Mountbatten for further info on threat models

https://www.owasp.org/index.php/Application_Threat_Modeling https://github.com/stevespringett/threatmodel-sdk

Company Security Champion Programs

- Why?
  - Better code coverage
  - Greater visibility
  - Improve security culture

Gaining Better Code Coverage

- 3-6% ratio of security eng’s to development eng’s 😱
- Security cannot cover enough ground. Needs deputies.
- Training (in specific tools and process) is key
- Use the release tooling you have to measure the coverage

http://www.infosecisland.com/blogview/8327-How-Many-Information-Security-Staff-Do-We-Need.html

How can your company start a Security Champions program?

0. Pick a name

1. Identify the Security Manager

2. Decide how to divide up Champs… by product, scrum team, BU, etc.

3. Define responsibilities clearly

4. Train and empower and track progress

5. With Maturity, increase incentives for better adoption

0. Pick a Name

Choose a metaphor that can guide your structure and has meaning in your culture

1. Identify the Security Manager

- The Program Owner of the program
    - An Application Security Engineer or a Community Manager
- Either works directly with Security Champions or works on a pyramid of Sec Engs depending on org size
- Also identify security team partners to build the pyramid if needed

2. Divide up the Champs

- Security Champions will divide and conquer
    - Based on a manageable unit of ownership
- BU for Startup, Product/Application for Midsize, Scrum team for large Enterprise
- Think 1:<15 ratio SecChamp:SecMgr is best, 1:30 is almost impossible, break it into smaller pods of Sec Champs and Security Team partners to get large numbers covered

3. Define EVERYTHING

- Make it as official as possible
- Define responsibilities clearly
    - Required security training curriculum
    - Threat modeling diagram maintenance
    - Security testing with SAST scanner and more defined tools
    - Required awareness communications and announcements in standup
    - Might also document what it’s NOT if there are FAQ’s. (e.g. It is NOT a risk acceptance or “security sign-off” role.)
- Bubble up recognition for everyone involved

4. Train Empower Track

- Train for Intermediate level secure coding skills and threat modeling concepts
- Empower with the appropriate set of tools
  - SAST
  - SCA
  - SAST & security plugins in the IDE
  - Burp Suite for reproducing pentest results
- Feel free to automate everything! (Jeeeeenkins!!)
- Track work metrics with bug tracker tags and surveys/1:1's with security mgr

5. Plan Maturity

- It's good to start with a pilot, but pilots must have defined ends. Then scale towards 100% adoption.
- Start with teams that fit the mold, but then expand to edge cases and remote offices. Strong documentation will allow the edge case to not become exceptions. Nothing will replace facetime.
- Then don't forget to add incentives/rewards package. This is not an intern program. This is not free work. These are your *most* skilled workers becoming more valuable. Grab every incentive your company culture can allow.

Takeaways

- Transform an interest in security into a role enhancement
- Start testing with low hanging fruit and move security activities left in the SLDC
- Many different types of programs, but all are clearly defined and supported by leadership
- The security team needs YOUR help! Accept the call!
- Contact: @dewzi or Marisa.Fagan@Synopsys.com