Who are you?
What’s the problem?

• Microsoft & Cisco leading by example
• Developers don’t believe SQLi is real
• Managers only care about time to market
• Compliance diverts attention from risks
Is there a solution?

• Before you begin:
  • Know what you can do
  • Know how much you can spend
  • Know who you have

• Do we need another secure coding program?
Rogue Secure Development

Phase 1: Template
Phase 2: Gauntlet
Phase 3: Code Review
Phase 4: Sanity Check
Phase 5: Release
Phase 0: The Incident

- A realistic approach
- Begin with a breach
- Initiate Incident Response Plan
- Now, let’s stop that *kind* of bug from happening again
Phase 1: The Template

- Types of software and bugs
- Choose the template
- Is this right for you?
- Build Requirements Document

Example: Apple iPad registration exposed on web
Phase 2: The Gauntlet

- Bring up QA testers
- Run automated security tools that search code for common bugs
- Use the Common Bugs list
- Pass to the Coders for remediation

Example: Adobe strcat
Phase 3: The Code Review

- Coders check the list
- Fix the Highs and the Lows
- Code Managers check the Coders
- Unit tests in isolation
- Remediation

Example: Perl URL directory traversal attack
Phase 4: The Sanity Check

- QA - Classic functionality test
- QA - Verify the known bugs have been patched
- Defense in Depth
- SE - Sign off for release OR send back to coder for Phase 3

Example: Windows DLL Preloading Attack
Phase 5: The Release

- PM - Hand off product to Marketing/Distribution
- PM - Edit SDLC to learn from the process
- Attempt to make less "top 20" mistakes next time

Remember: Focus on the incident
Example: Apple Quicktime "_MARSHEALED_PUNK" backdoor
But why?

• Maybe this isn’t right for you
• If it is,
  • You save money
  • Better code
  • Customers expect it
  • Stay off the headlines
The future

• Doesn’t look good
• Hackers always one step ahead
• Can’t be secure “once and for all”
• Low Hanging Fruit
• Reduce spending!
Questions/Comments?

- Marisa Fagan can be reached at:
  - marisa@erratasec.com
  - Twitter: @errata @dewzi
  - http://erratasec.blogspot.com
  - http://erratasec.com
  - http://erratasec.com