Training Modules for Writing Secure Software

PI: Doug Jacobson (dougj@iastate.edu)
Researcher: David Koster
Training Goals

• Address OWASP top 10 vulnerabilities
• Engaging training methodology
• Understand the attacker’s philosophy
• Maintain records for compliance purposes

• Produce measurably fewer defects
Training Structure

• ½ Day Modules
• Single exploit focus
• Designed for small groups
• Self guided
  • Educational text & references
    • Internal company bug reports / material
  • Attack & Defend exercises
Training Structure

- Education
- Explore
- Defend
- Attack
- Review

IOWA STATE UNIVERSITY

Computer Engineering
Framework

- Google App Engine
  - Python
  - webapp2 / Django
- Independent Modules
  - Allows removal of proprietary information
  - Internal evaluation & grading mechanism
Project Excerpt - CSRF

• Explore
  • Find the CSRF token
  • When does it change?
  • Where is it stored?
  • What happens when it is changed?
  • When it is omitted?

• The exploring section is designed to mimic the types of questions we want asked during dev
Project Excerpt - CSRF

- Attack – Page w/o CSRF Protection
- Attack – Page w/ CSRF
  - Spawn independent sessions
  - Steal CSRF token
  - Submit a page from a different session

- The attacks are about illustrating the scope of the exploits and the prevention mechanisms
Project Excerpt - CSRF

- Defend
  - Write your own implementation

OR

- Review the framework implementation

- Produce exploit free page
Project Excerpt - CSRF

• Review
  • Impact assessment
  • Relevance
  • Limitations of counter measures
  • Detection of exploits
Full Topics List

- XSS
- CSRF
- Encryption
- SQL / GQL Injection
- Authentication
- SSL / Session Management
- Data Leaks
- 32 Planned Exercises
Future

• Deeper technical topics
• Architecture specific exploits
• Multi-stage exploits