About Me

- [www.voixsecurity.blogspot.com](http://www.voixsecurity.blogspot.com)
- [Larry.Conklin@owasp.org](mailto:Larry.Conklin@owasp.org)
- Twitter @lwconklin
Agenda

• The most important side in this deck…
• Why…
• The most important people…Contributors
• Leaders
• Current Focus…(We need you)
• Next Steps…
• The second most important slide in this deck…
https://www.owasp.org/index.php/OWASP_Code_review_V2_Project

https://www.owasp.org/index.php/OWASP_Code_review_V2_Table_of_Contents

OWASP is serving that need.
• Larry Conklin
• Johanna Curiel
• Eoin Keary
• Islam Azeddine Mennouchi
• Abbas Naderi
• Carlos Pantelides
• Ashish Rao
• Gary David Robinson

• Colin Watson
• Mghazli Zyad
Co-Leaders

• Eoin Keary

• Larry Conklin

With a great amount of support from Samantha Groves
Where we are at... Pre-Alpha Release...

• Finishing content. Begin reviewing for spelling, grammar and technical accuracy.

• Afterwards our steps will be to have book reviewed by a professional editor, and review graphics with a professional graphics designer.
AppSec USA 2013

- 360 Reviews
- Code Review Approach
- Application Threat Modeling
- Code Layout Design Architecture
- SDLC Integration
- Secure Depending Configuration
- Metrics Code Review
- Source Sink Review
- Code Review Coverage
- Code Review Compliance
- Authentication Controls
- Authentication
- Out of Band
- Reducing Attack Surface
- File Resource Handling

Hosted by OWASP & the NYC Chapter
- Client Side Code
  Introduction, json, Content Security, Browser Defense Policies
- Input Validation
  Introduction, Regex Gotchas, ESAPI
- Resource Exhaustion
  Error Handling, Native Calls

- Logging Code
- Security Alerts
- Secure Storage
- Persistent AntiPattern
  Introduction, Ruby, PHP
- Reflected AntiPattern
  Introduction, Ruby
- Stored AntiPattern
  Introduction, PHP, Ruby

Hosted by OWASP & the NYC Chapter
• JQuery Mistakes
• Review Code SQL Injection (.Net, HQL(Hibernate))
• AntiPattern, PHP, Java,.Net,ColdFusion
• Transactional logic / Non idempotent functions / State Changing Functions

• Reviewing code for poor logic /Business logic/Complex authorization
• Secure Communications, HTTP Hdrs, HTTP Hdrs CSP,HTTP HSTS
• Tech Stack Pitfalls
• Framework Specific Issues...
• Looking for volunteers to begin word smiting, checking for technical accuracy, adding content.

• Mailing lists…

http://lists.owasp.org/mailman/listinfo/owasp-codereview

http://lists.owasp.org/mailman/listinfo/owasp_code_review_guide_authors
• Questions….