Application Security and Audit

Presented to: ISACA – Houston Chapter
January 21, 2010

Getting Buy-In

- Emphasize the win-win nature of security
  - You're not out "to get" anyone
  - Goal is to protect employee and customer data, comply with regulations, and stay out of the headlines

High Level Areas

- Identify the “risk profile” of the app
- Review the architecture
- Authentication and authorization
- Auditing and logging
- Data validation
- Error Handling
- Cryptography

Vulnerabilities

- OWASP Top 10
  - Lists the most serious web application vulnerabilities
  - Latest version is 2007 (2010 rc1 released)
- 2009 CWE/SANS Top 25
  - Insecure Interaction Between Components
  - Risky Resource Management
  - Porous Defenses

Static Code Scanning

- Helps with the identification of coding errors by automating the scanning of source code
- Must validate findings to identify false positives
- Logic errors are still a manual process

Free Tools

- Burp
- DHTML debugging
  - Dom Inspector
  - WebDeveloper
  - Firebug
- HTTP traffic analysis
  - LiveHTTPheaders
  - ModifyHeaders
  - TamperData
  - WebScarab
- XSS ME and SQL Inject ME

Challenges

- Gaining trust
- Communicating risk
- Following up with remediation actions (workflow)
- Sustainability

Objectives

- Get appsec integrated into the project management lifecycle.
- Ensure that the same mistakes are not being made over and over.
- Improve the ability of applications to pass audits.

Comments? Questions?

Email: mark.adams3@halliburton.com