Web Application Security Assessment Policy

John Hally

John.hally@comcast.net

Why This Policy?

- Limit attack surface of our web applications
- Web application flaws/vulnerabilities are a major attack vector
- Protect Company Brand/Reputation
- Enterprise Security Policy Compliance
- Other Compliance Requirements

Policy Applicability

- All web applications - internal, external, 3rd party
- Project Managers - Scheduling
- Security Engineering – Reporting and recommendations
- Development Team – Code remediation
- Chief Information officer – Final authority

Assessment Criteria

- **New or Major Application Release** – Subject to a full assessment
- **Third Party or Acquired Web Application** – Subject to full assessment
- **Point Releases** – Subject to an appropriate assessment level based risk of changes
- **Patch Releases** – Subject to an appropriate assessment level based on the risk of changes to functionality
- **Emergency Releases** – Special case that will forgo an assessment, will require CIO approval

Risk Rating

- Risk calculation based on OWASP Risk Rating Methodology
- High – must be fixed before release
- Medium – fix in patch release unless cumulative risk becomes too high; other mitigation allowed
- Low – fix in point release

Non-compliance Ramifications

- Application may be taken offline
- Application functionality may be limited to temporarily mitigate issue (if possible)
- Denial of release into live environment