Application Security

■ Agenda

- Threats Landscape
- Application Threats
- Survey Samples
- Secure SDLC Process
- Security _ Non functional requirements
- Mitigation
- Awareness Level
- Role of OWASP
Threats Landscape

- Non availability of resources, Data integrity loss, loss of confidentiality of sensitive information
  
  - Attack can be directly on to the information
  - Attack can be through application vulnerability
  - Attack can be internal
  - Attack can be from outside
  - Attack can be compromising the IT infrastructure
  - Attack due to Natural Disaster/Man made disaster
Application Threats

- Social Engineering
- Non segregation of Duties
- Improper Control Validation
- Improper coding
- Improper Security Testing
- Non availability/ non execution of compensating controls
Confidence in house developed applications

- A majority of applications in use at our organization are commercial off-the-shelf applications. 23%
- Not at all confident - we haven’t done enough to assess and mitigate vulnerabilities. 20%
- Somewhat confident - we haven’t had any issues to date. 35%
- Very confident - we’ve assessed our risks and tested our security. 22%
Confidence in third party applications

- Not at all confident - they haven't done enough to assess and mitigate vulnerabilities: 21%
- Somewhat confident - we haven't had any issues to date: 60%
- Very confident - they've assessed their risks and tested their security: 19%
Reasons for not adopting Secure Coding Practices

Reasons for Not Adopting

- Not aware of methodologies
- Too expensive
- Requires too many resources
- Too time consuming
- Deemed unnecessary
- Other
- Blank
Driven by PCI DSS Compliance

5. In your recent experience, how much of an organization's Web application security program is driven by PCI-DSS today?

<table>
<thead>
<tr>
<th>Response</th>
<th>Response Percent</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lot (otherwise we'd do nothing)</td>
<td>19.1%</td>
<td>57</td>
</tr>
<tr>
<td>Influenced somewhat</td>
<td>47.3%</td>
<td>141</td>
</tr>
<tr>
<td>Little to none</td>
<td>33.6%</td>
<td>100</td>
</tr>
</tbody>
</table>

- comments: 40
- answered question: 296
- skipped question: 42
Secure Software Development Lifecycle

Verification & Validation

Requirements
- Non-Functional Review (NFR)
- Customer sign off
- Security requirement review
- Architecture design review
- Customer Sign off

Design

Construction

Testing
- Testing for Non-Functional Review (NFR)
- Web application security testing

Delivery
- Application Audit
- Web Application Security Testing

Configuration Management Process
Security- Non Functional Requirements

- Validations (input, Processing, Output)
- Identification & Authentication
- Entitlements
- Operational Configurations
- Implementation Configurations
- Audit Trail
- Segregation of Duties
Mitigation

- Application Security as part of Enterprise Risk Management Program
- Design Review
- Code review using coding standards
- Security Testing as part of System Testing
- Application Audit at frequent intervals
- Application weaknesses to be compensated by administrative controls
Application Audit - Definition

- Business Process
  - Inputs
  - Process
  - Output
  - Logical Security
  - Third party Services
  - Administration
  - Audit Trail

- Application
  - Web Vulnerability
  - Application Acquisition
  - Change Management
  - User Support

- Infrastructure
  - Vulnerability Assessment
  - Potential Testing
  - Business Continuity
  - Licenses

- Data
  - Change Management
  - Access Control
  - Audit Trail
  - Archival
Awareness Level

- It is at minimum and slowly improving
- Should be encouraged through forums like ISACA, OWASP, CLASP etc.
- Security Testing should be mandated as part of SDLC framework
- Training, workshop on continuous basis on new threats and mitigation
OWASP Role

- Should be lauded for pioneering in this area

- Collaborate with other organizations like ISACA, CSI to reach more people
Q & A