Building Secure Web Applications In a Cloud Services Environment

Misha Logvinov
Alex Bello
IronKey, Inc.

OWASP
July 1, 2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.
Who are we?

Misha Logvinov
- VP of Online Operations at IronKey
- Director of Operations at Yodlee

Alex Bello
- Director of Technical Operations at IronKey
- Product Threat Team Lead at IronKey
- Technical Operations at Anti-Phishing Working Group (APWG)
Reality check

- The Internet is full of web application hacking tools and tutorials
- Botnets are used to scan for recent web app exploits
- 75% of attacks happen at the app layer
- Majority of web app vulnerabilities remain undetected
- App security is an after-thought for most of the Internet-enabled businesses
- Security holes in web apps result in large business losses
- Bad guys are getting smarter and are not sitting still
Who gets attacked

- Brick and Mortar Retail
- Healthcare
- Government
- Small businesses
- Web 2.0
Who attacks

- Kids playing war
- Researchers looking for fame
- Organized crime
- Competition
- Governments
Consequences

- Customers defect
- Brand damaged and stock price plummets
- Large fines
- Company out of business
- You may get fired
How?

- The most widespread vulnerabilities in web apps (Source: projects.webappsec.org):

![Vulnerability Chart]

- Attacks on the rise: SQL Injection, File Inclusion, Web Server Intrusion (Source: zone-h.org)
- OWASP Top 10 Most Critical Security Risks
Recent breaches

December 2009

SQL injection vulnerability, no encryption of critical data, insufficient security monitoring, poor handling of disclosure

Consequences
PR nightmare
Class-action lawsuit
Recent breaches

April 2010

Insufficient security testing and monitoring

Consequences
PR nightmare

Blippy suffers credit card number leak

26 April 2010

Shoppers’ social networking service Blippy suffered a security flaw late last week, after some of its users’ credit card numbers began appearing in search results.
Recent breaches

June 2010

Personally Identifiable Information was displayed without proper authentication, insufficient output monitoring, “great” exploit timing

Consequences
PR nightmare
Security researcher gets arrested on drug charges
Why

Insufficient Security in:

- SDLC
- Web Operations
How to get started?

- Understand business, security and privacy requirements
- Assess important security controls
- Create security awareness and facilitate training
- Get release management under control
- Scan applications prior to new releases
- Benchmark against industry best-practices
- Create and communicate meaningful metrics
- Conduct independent security assessments
Doing things right in the long run

- Implement a formal security program
- Integrate security into Software Development Life Cycle (SDLC)
- Make security a competitive advantage for your business
Implement a formal security program

- Security framework
- Policies and procedures
- Training
- Coding standards
- Risk assessments
- Security testing and evaluation
- Reporting
- Incident response
- Change management
Integrate security into SDLC

2. Design

- Security requirements
- Threat modeling
- Secure architecture design
## Threat matrix example

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threats</th>
<th>Security Controls</th>
<th>Threat Priority</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1</td>
<td>Threat 1</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 2</td>
<td>Threat 2</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 3</td>
<td>Threat 3</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 4</td>
<td>Threat 4</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 5</td>
<td>Threat 5</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 6</td>
<td>Threat 6</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 7</td>
<td>Threat 7</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 8</td>
<td>Threat 8</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 9</td>
<td>Threat 9</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 10</td>
<td>Threat 10</td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Category 11</td>
<td>Threat 11</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 12</td>
<td>Threat 12</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 13</td>
<td>Threat 13</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 14</td>
<td>Threat 14</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 15</td>
<td>Threat 15</td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Category 16</td>
<td>Threat 16</td>
<td></td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

**Threat/Control Ranking**

- 9 - Strong
- 6 - Moderate
- 3 - Weak, works better in combination with other Weak or Moderate
Integrate security into SDLC

3. Development

- Use modern frameworks
- Develop secure coding standards
- Secure implementation, best practices and checklists
- Code review (internal/third party)
- Static code analysis
Integrate security into SDLC

3. Quality Assurance

- Security testing of changes (automated/manual)
- Regression testing
- Bug tracking integration
Integrate security into SDLC

4-5. Operations

- Infrastructure hardening
- Vulnerability alerting
- Web application firewalls
- Security events alerting & analysis
- Automated infrastructure testing
- Penetration testing (internal/third party)
- Tracking security metrics
- Change & release management
Hardening

- CIS and NSA hardening guidelines

- OWASP Backend Security Project

- Automated open-source and commercial tools
Standards & checklists

- OWASP Application Security Verification Standard Project
  

- The OWASP Code Review Top 9
  
Web app assessment initiatives

**Web app scanners**
Evaluation & Deployment: 6-8 weeks
Sample Budget: $20-50K

**Static source code analysis**
Evaluation & Deployment: 8-12 weeks
Sample Budget: $50-100K

**Web app firewalls**
Evaluation & Deployment: 6-8 weeks
Sample Budget: $25-100K+
Rules of thumb

- Invest in security training and certification of core personnel
- Encrypt all sensitive data and pay attention to key management
- Never trust input, validate all input/output
- Harden your systems
- Tightly control who has access to your environment
- Stay on top of vulnerabilities and keep your networks, servers and applications up-to-date
Conclusions

- Integrating security into SDLC from the beginning is worth it! Shortcuts will cost more time and $$ later
- Rome wasn’t built in a day – take a phased approach
- Mold a security framework around your business, not the other way around
- Don’t underestimate the power of marketing security within your organization
Q & A