Our Vision for Application Security

David Ng
Rational Software Security, Asean
IBM Software Group
Agenda

- Application Security Defined
- Hacking Example
- Trends and Best Practices
- IBM Vision and Roadmap for Application Security
The world is riskier than it used to be…

Massive insider breach at DuPont
February 15, 2007
By: Larry Greenemeier

TJX data breach: At 45.6M card numbers, it’s the biggest ever
March 29, 2007
By: Jaikumar Vijayan

Black Friday Turns Servers Dark at Walmart, Macy’s
November 25, 2006
By: Evan Schuman

Blackberry outage widespread
February 14, 2007
By Marcia Walton

Bill would punish retailers for leaks of personal data
February 22, 2007
By Joseph Pereira
Evolving Threats
Application Security - Understanding the Problem

Info Security Landscape

Desktop
- Antivirus Protection

Transport
- Encryption (SSL)

Network
- Firewalls / IDS / IPS

Web Applications
- Application Servers
- Backend Server
- Databases
- Web Servers
Hackers Exploit Unintended Functionality to Attack Apps
Application Security Hacking Example
Web applications and web services are prone to attack so effective security and compliance are required

- 75% of today’s attacks occur at application layer
  - Yet only 10% of corporate spending is allocated to web application security
  - 80% of organizations will experience an application security incident by 2010

Vulnerabilities are growing at an alarming rate
SQL Injection

- User input inserted into SQL Command:
  - Get product details by id:
    Select * from products where id='+ $REQUEST["id"]';
  - Hack: send param id with value ‘ or ‘='''
  - Resulting executed SQL:
    Select * from products where id='' or ''='' 
  - All products returned
Online Banking Login

Username: 
Password: ****

Login
An Error Has Occurred

Summary:

**Syntax error (missing operator) in query expression 'username = "" AND password = 'asdf'.**

Error Message:

```
```
Hello, John Smith

Welcome to Altoro Mutual Online.

View Account Details: 1001160140 Checking GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.

Copyright © 2007, Watchfire Corporation. All rights reserved.
Motives Behind Application Hacking Incidents

Source: Breach/WASC 2007 Web Hacking Incident Annual Report
Growth In Browser Vulnerabilities

Source: IBM Xforce 2007 Annual Report
What is the Root Cause?

1. Developers not trained in security
   - Most computer science curricula have no security courses

2. Under investment from security teams
   - Lack of tools, policies, process, etc.

3. Growth in complex, mission critical online applications
   - Online banking, commerce, Web 2.0, etc

4. Number one focus by hackers
   - 75% of attacks focused on applications - Gartner

Result: Application security incidents and lost data on the rise
Where Do These Problems Exist?

Type:
- Customer facing services
- Partner portals
- Employee intranets

Source:
1. Applications you buy – e.g. COTS
2. Applications you build internally
3. Applications you outsource
Application Security Maturity Model

- **UNAWARE PHASE**: 30%
- **AWARENESS PHASE**: 30%
- **CORRECTIVE PHASE**: 30%
- **OPERATIONS EXCELLENCE PHASE**: 10%

Duration: 2-3 Years
Building Security Into the Development Process

**Define/ Design**
- Continuous security education of architects, developers etc. on Web Application Security

**Development**
- Test apps for security issues in Development identifying issues at their earliest point
- Realize optimum security testing efficiencies (cost reduction)

**Production**
- Test existing deployed apps
- Eliminate security exposure in live applications

**Deploy**
- Test apps before going to production
- Deploy secure web applications

**Test**
- Test apps for security issues in QA organization along with performance and functional testing
- Reduce costs of security testing
Security Testing Within the Software Lifecycle

SDLC

Coding

Build

QA

Security

Production

Developers

Developers

Developers

Application Security Testing Maturity
IBM Vision and Roadmap for Application Security
IBM Security Framework

The IBM Security Framework

- Security Governance, Risk Management and Compliance
- People and Identity
- Data and Information
- **Application and Process**
- Network, Server, and End-point
- Physical Infrastructure

Common Policy, Event Handling and Reporting

External Representation

- **Professional Services**
- **Managed Security Services**
- **Security Hardware and Software**

- Security Governance, Risk & Compliance Solutions
- Identity and Access Management Solutions
- Information Security Solutions
- Application Security Lifecycle Mgmt Solutions
- Threat and Vulnerability Mgmt & Monitoring Solutions
- Physical Security Solutions
IBM is laying the foundation for end-to-end application security

- IBM Global Services – security risk assessments helping define policies and processes
- Rational – automated vulnerability testing for web applications/web services across the development cycle
- IBM Technology Services/ISS – managed services for network and application vulnerability assessment
- Tivoli – access control and security information and event management to web applications/web services
- DataPower – provides SOA security solutions
- IBM Research – static analysis technology

Application Security Management Lifecycle

1. Define Policy
2. Build & Test
3. Deploy
4. Manage, Monitor & Defend
5. Continuous monitor applications for vulnerabilities and defend against attacks
6. Configure infrastructure for application policies; deploy applications in production
7. Build security into application design and model threats
8. Build and test individual and composite applications
9. Continuously monitor applications for vulnerabilities and defend against attacks
10. Configure infrastructure for application policies; deploy applications in production
Software Security Development Ecosystem

Control, Monitor and Report

- Developers
- Build System
- Quality Assurance Testing
- Security Auditor scanning

Coding  Build  QA  Security

Web Based Security Training
IBM Rational AppScan SDLC Ecosystem

IBM Rational AppScan Enterprise / Reporting Console

- **AppScan Developer Ed** (Eclipse IDE)
- **AppScan Ent. QuickScan** (web client)
- **Rational BuildForge**
- **AppScan Developer Ed for build systems** (scanning agent)
- **Rational ClearQuest**
- **AppScan Tester Ed** (scanning agent)
- **Rational Quality Manager**
- **AppScan Tester Ed** (QA client)
- **AppScan Enterprise user** (web client)
- **AppScan Standard Ed** (desktop)

**Build**

- Automate Security / Compliance testing in the Build Process
- Security / compliance testing incorporated into testing & remediation workflows

**Code**

**Build**

**QA**

**Security**

- Security and Compliance Testing, oversight, control, policy, in-depth tests

IBM Rational Web Based Training for AppScan

RSDC Geo Review
Rational AppScan: Find and fix web application security and compliance issues
Security Testing is managed just like other types of testing.
Forthcoming AppScan DE

- Security Testing in your Development Environment (Architect, RAD or Eclipse)

- Integration with source code, WebSphere, ClearQuest

- Can interoperate with AppScan Enterprise for central licensing, permissions and oversight
AppScan Enterprise – Dashboards and Metrics
Integrated Computer Based Training

Key to adoption across the organization is education

- Self-service – more convenient than traditional training
  - Participants no longer have to schedule time “out of the office”

- Self-paced – greater information retention
  - With digestible content modules, participants no longer experience information overload

- Just-in-time reference-ability
  - Full access to searchable, online content for 12 months

- Structure
  - Courses are individual modules
  - Typically 15 minutes or less
QUESTIONS