Building a Security Ecosystem

Robert Fly
VP, Product Security
salesforce.com

Salesforce.com Customers

92,300+

Paying Customers

Intro to AppExchange

AppExchange

1100+ Applications
Composite, Native, Client
780,000+ Installs
Security Reviews
Listing Fee

Security Review

~12 month review cycle
Automated & Manual Assessments
OWASP/WASC checks
Requirements for what to fix and how quickly

Agenda

What we did and why?

Force.com Secure Cloud Development

Vision Build an ecosystem and community of developers who hold trust as their top value.

Why?

75% | 86% | ???

Gartner

force.com™
platform as a service

Developer Security Savvy?

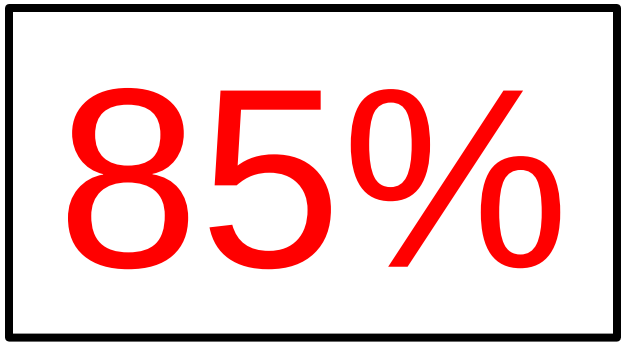
25%

40%

60%

75%

Fail Rates



composite

native

Leader in this space

- “Salesforce gets a gold star” – Alex Stamos (Founder iSEC)

Secure Building Blocks

Auth, Session Handling, Filtering, SSL, Infrastructure, Patching, Auditing & Logging

Default Protections

XSS, CSRF
Separate Domains
PAC

Where did we focus…

Easy - Free - Transparent

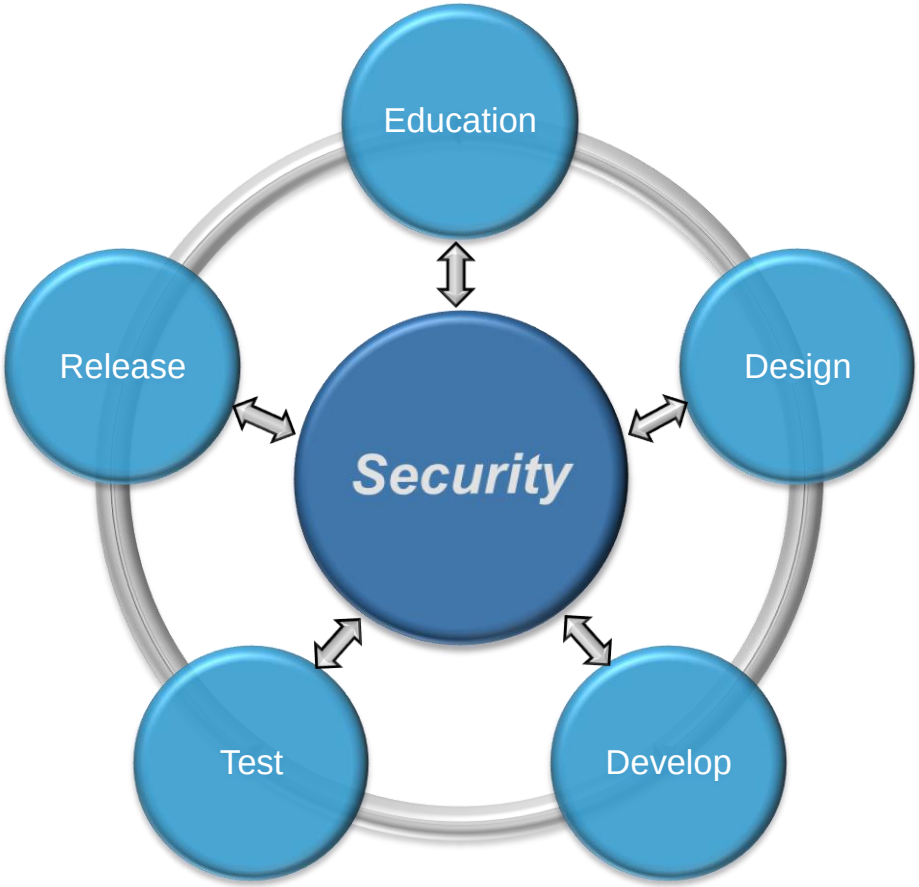
Partnered With…

Product Management and R&D
Alliances
Developer Evangelists
AppExchange Team
Training and Certification

Developer Experience

Integrated into Force.com (not OWASP)
Focus 100% on 80%
Usable
Align incentives
No cost

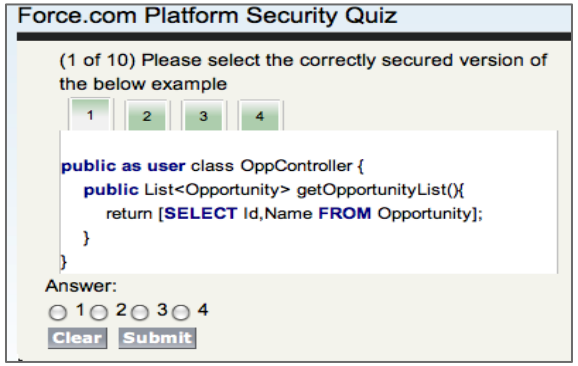
Force.com Secure Cloud Development



Seamless integration of security into your existing SDLC

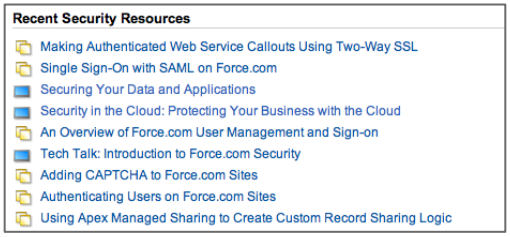
(Secure) Education

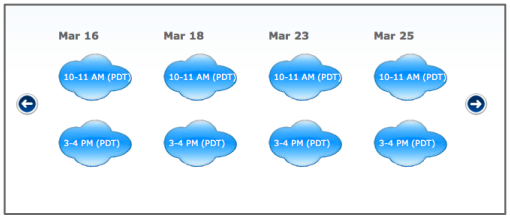
- **Overview of Force.com Security**
  - Learn about the sharing model and various security controls available to org administrators
- **Writing Secure Apps (online)**
  - Get educated on writing secure code on Force.com
- **Developer Quiz**
  - Assess your security awareness and learn to identify vulnerabilities within Force.com code
- **Security Blog and Twitter**
  - Consistent updates on our latest security research, contests and more.



(Secure) Design

- **Security Resources**
  - Generic Force.com articles and resources. Topics include SAML, sharing, etc.
- **Security Self-Assessment**
  - Receive a customized report with links to security articles and resources specific to your application architecture
- **Office Hours**
  - Receive free consultation from a member of the salesforce.com security team
- **Security Discussion Board**
  - Community based forum for answering security questions





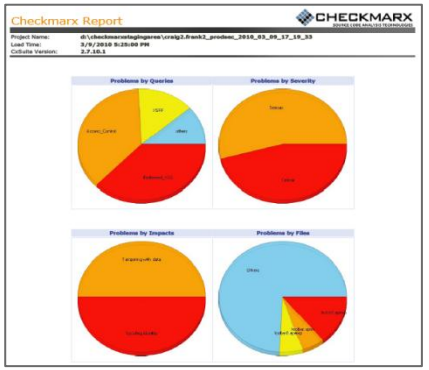
(Secure) Development

- **Secure Coding Guidelines**
  - Obtain platform-specific (Force.com, Java, .Net, etc.) recommendations on mitigating security vulnerabilities such as XSS, Injection, Session Management, etc.

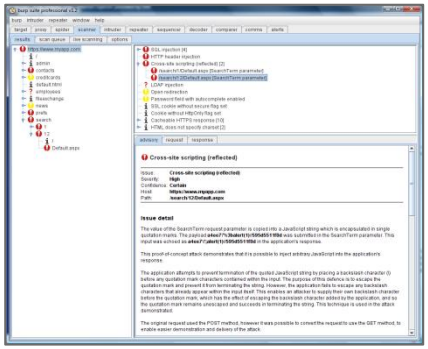
- **Secure Coding Library**
  - Open source library for implementing additional security features (CRUD/FLS, input validation, output encoding, etc.)
  - Part of OWASP Enterprise Security API

(Secure) Testing

- **Force.com Source Scanner**
  - On-demand static source code analysis tool to help identify potential vulnerabilities and code quality issues within your Apex and Visualforce code



- **Web Application Security Scanner**
  - Integrating a web applications with Force.com? AppExchange partners receive a free license for Burp Suite Professional



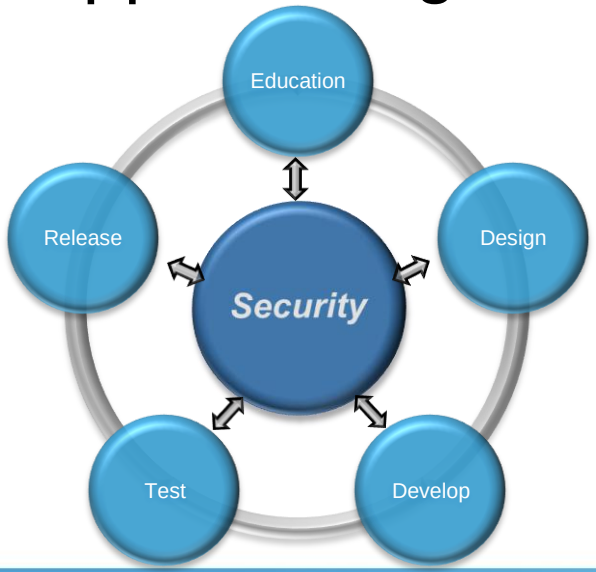
(Secure) Release

- **Salesforce.com Security Review**
  - Periodic security review of AppExchange and OEM applications
  - Details published at: http://wiki.developerforce.com/index.php/Security_Review

- **Incident Response (Coming Soon)**
  - Guidance on engaging with customers and salesforce.com in case of a security incident

Force.com Secure Cloud Development

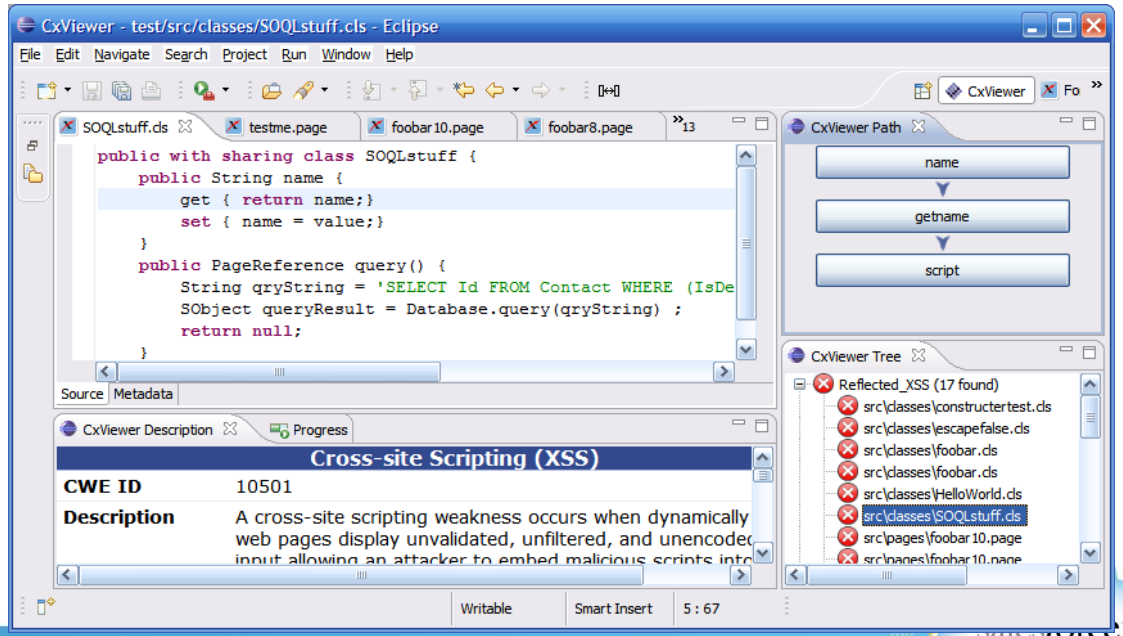
- Free, ready to “consume” resources
- More secure Force.com ecosystem
- Reduced development costs
- Streamlined AppExchange security process



One More Thing…

Force.com Eclipse Code Scanner

- Direct visibility into security and quality issues
  - Eclipse Plugin
  - Line by line click-through
- Offered by Checkmarx



Are we any better?

Stats

- 10000+ code bases scanned
- 183 Million Lines of Code Scanned
- 280,000+ issues identified by the scanner
  - ~80% accuracy rate
  - 55/45 split between security and quality, respectively

Positives

- I *heart* the security scanner. Use it with every project.
- Have u run the #Salesforce Security Scanner today? It's like Old Spice for your apps. Be fresh, secure and confident!
- Don't forget to run the free code scanner. It's soooo helpful for writing secure #salesforce code
- Using Eclipse/Force.com Ide … #loveTheScanner
- Awesome to see @salesforce respond to customer needs via twitter. Security Review team has been fantastic. Great work @benioff and team.

Positives

19%

native

50%

composite

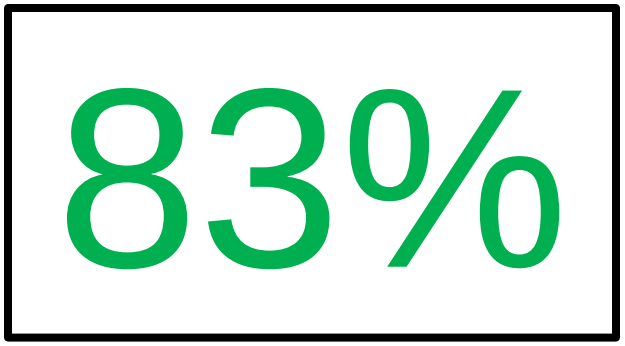
203

24 hours

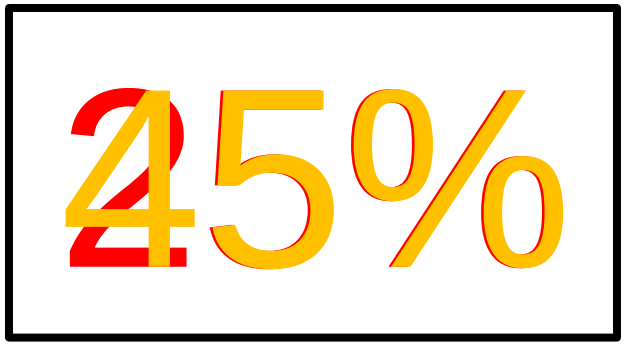
437

over 3 months

Positives



improvement



quiz

Where To Focus Next

- Require issues to be addressed & auditing
- Better integration into product
- Improve composite app first time pass rate
- Other platforms
- Continued laser focus on quality

Key Take Aways

- http://developer.force.com/security

Question & Answer

salesforce.com **Robert Fly**