



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.

The OWASP Foundation

<http://www.owasp.org>

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

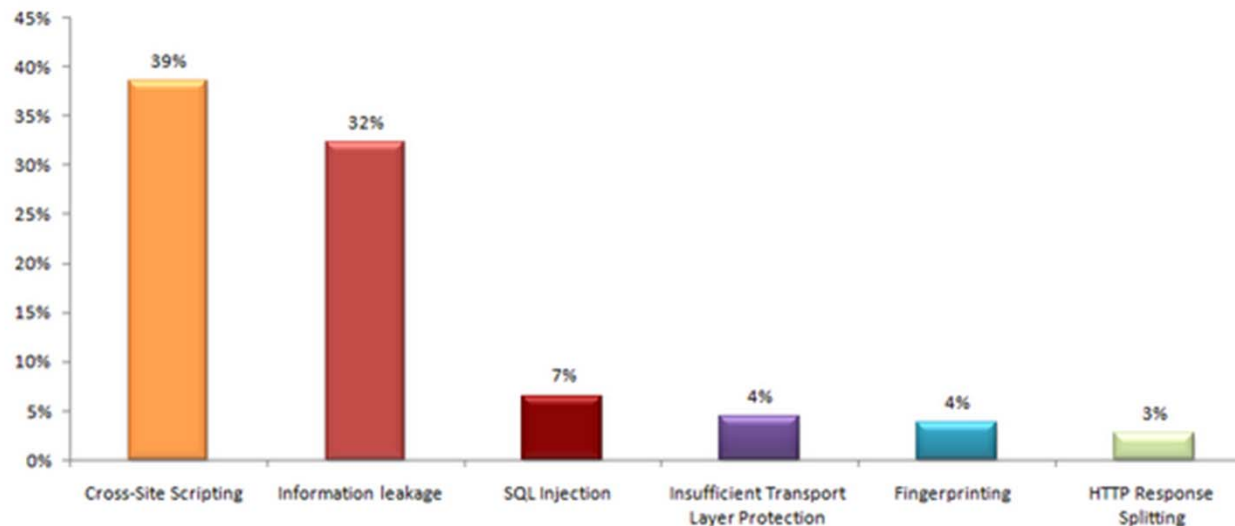
- Kids playing war
- Researchers looking for fame
- Organized crime
- Competition
- Governments

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):



- 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



The screenshot shows a news article on the Computerworld website. The page has a yellow header with the 'COMPUTERWORLD' logo and a 'Subscribe to a Newsletter' link. Below the header is a navigation bar with 'Topics', 'News', 'In Depth', 'Reviews', 'Blogs', 'Opinion', and 'Shark Tank'. A secondary navigation bar lists 'Security', 'App Security', 'Business Continuity', 'Cybercrime and Hacking', 'DRM and Privacy', and 'Security Hardware and Software'. The article title is 'RockYou hack exposes names, passwords of 30M accounts', with a sub-headline 'SQL injection flaw blamed for intrusion at social networking app vendor'. The author is 'By Jaikumar Vijayan' and the date is 'December 15, 2009 04:04 PM ET'. There are 8 comments and 14 recommendations. The article text begins with 'Computerworld - Hackers breached a database at social networking application maker RockYou Inc. and accessed username and password information on more than 30 million individuals with accounts at the company.'

Recent breaches

April 2010

Insufficient security testing and monitoring

Consequences
PR nightmare



The screenshot shows the website 'info security .com' with the tagline 'STRATEGY.INSIGHT.TECHNIQUE.'. The navigation menu includes 'Home', 'The Magazine', 'Advertising', 'Contacts', 'Links', and 'E-Newsletter'. A sidebar on the left lists various content types: Virtual Conference, Podcasts/ Newscasts, Webinars, Downloads/ White Papers, Blog, News, Application Security, Biometrics, and Business Continuity and Disaster Recovery. The main content area features a red header for 'News' and a news article titled 'Blippy suffers credit card number leak' dated 26 April 2010. The article text reads: '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

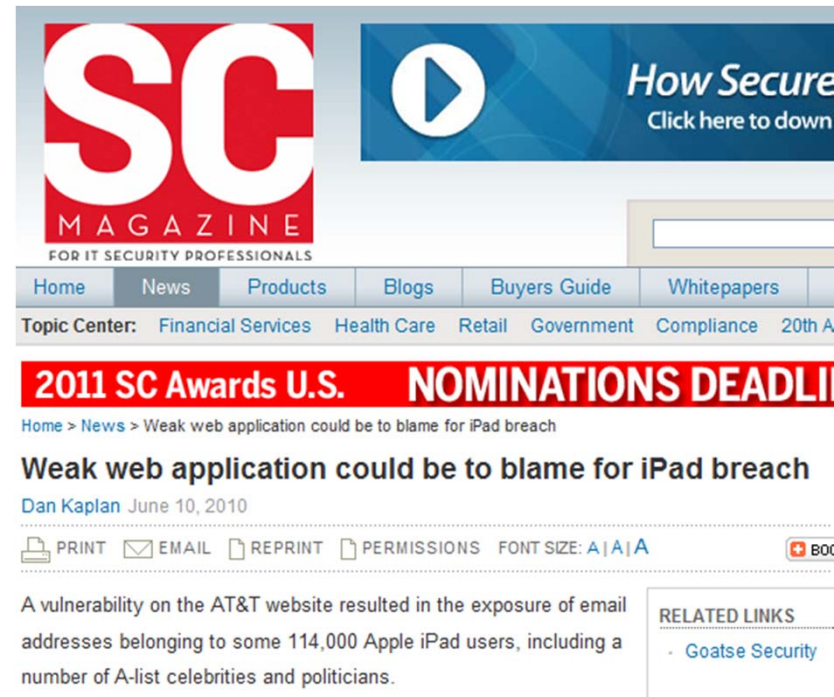
June 2010

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

Consequences

PR nightmare

Security researcher gets arrested on drug charges



The screenshot shows the SC Magazine website interface. At the top left is the SC Magazine logo with the tagline "FOR IT SECURITY PROFESSIONALS". To the right is a blue banner with a play button icon and the text "How Secure" and "Click here to down". Below the logo is a navigation menu with links for Home, News, Products, Blogs, Buyers Guide, and Whitepapers. A "Topic Center" section lists various industries: Financial Services, Health Care, Retail, Government, Compliance, and 20th A. A prominent red banner reads "2011 SC Awards U.S. NOMINATIONS DEADLI". Below this is a breadcrumb trail: "Home > News > Weak web application could be to blame for iPad breach". The main article title is "Weak web application could be to blame for iPad breach" by Dan Kaplan, dated June 10, 2010. Below the title are icons for PRINT, EMAIL, REPRINT, and PERMISSIONS, along with a font size selector (A|A|A) and a "BOX" icon. The article text states: "A vulnerability on the AT&T website resulted in the exposure of email addresses belonging to some 114,000 Apple iPad users, including a number of A-list celebrities and politicians." To the right of the text is a "RELATED LINKS" section with a link to "Goatse Security".

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

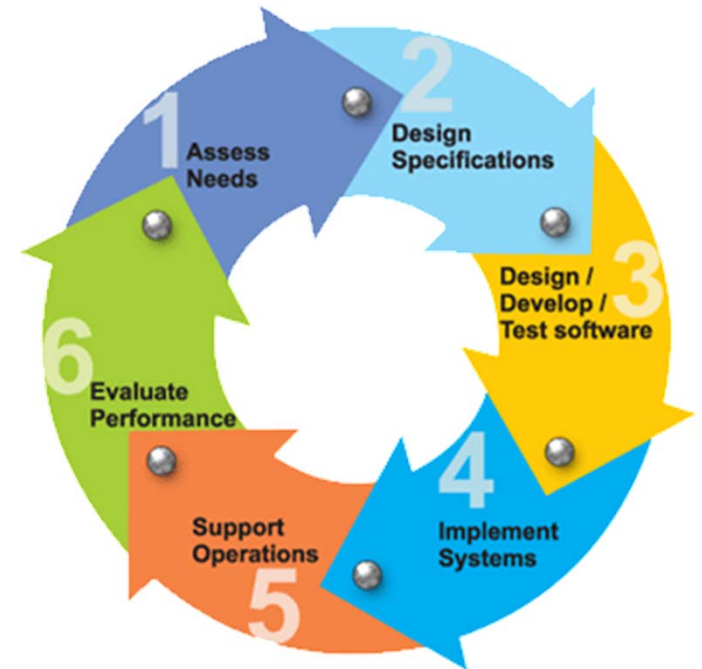
Implement a formal security program

- 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

		Security Controls																		
		Threat Priority	Software Version	Control 1	Control 2	Control 3	Control 4	Control 5	Control 6	Control 7	Control 8	Control 9	Control 10	Control 11	Control 12	Control 13	Control 14	Control 15	Control 16	Control 17
Threat Category	Threats																			
Category 1	Threat 1	5																		
Category 2	Threat 2	5																		
Category 3	Threat 3	5																		
Category 4	Threat 4	5																		
Category 5	Threat 5	5																		
Category 6	Threat 6	5																		
Category 7	Threat 11	5																		
Category 8	Threat 12	5																		
Category 9	Threat 14	4																		
Category 10	Threat 15	5																		
Category 11	Threat 16	5																		
Category 12	Threat 17	5																		
Category 13	Threat 18	5																		
Category 14	Threat 19	5																		
Category 15	Threat 20	5																		
Category 16	Threat 21	5																		

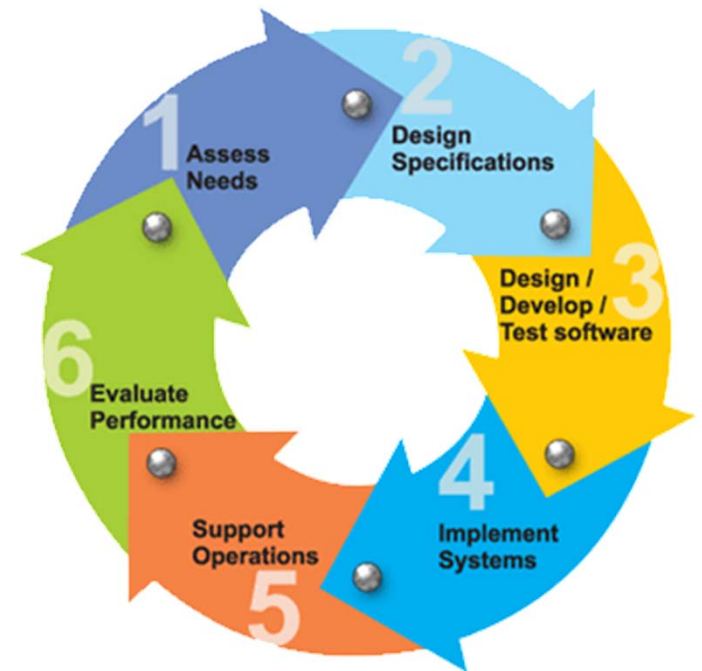
Threat/Control Ranking

- 9 - Strong
- 6 - Moderate
- 3 - Weak, works better in combination with other Weak or Moderate

Integrate security into SDLC

3. Development

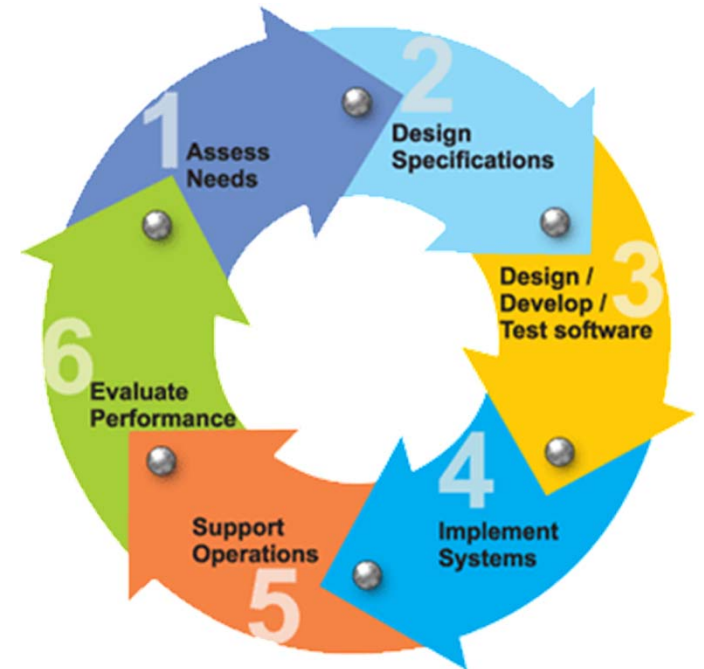
- Use modern frameworks
- Develop secure coding standards
- Secure implementation, best practices and checklists
- Code review (internal/third party)
- Static code analysis



Integrate security into SDLC

3. Quality Assurance

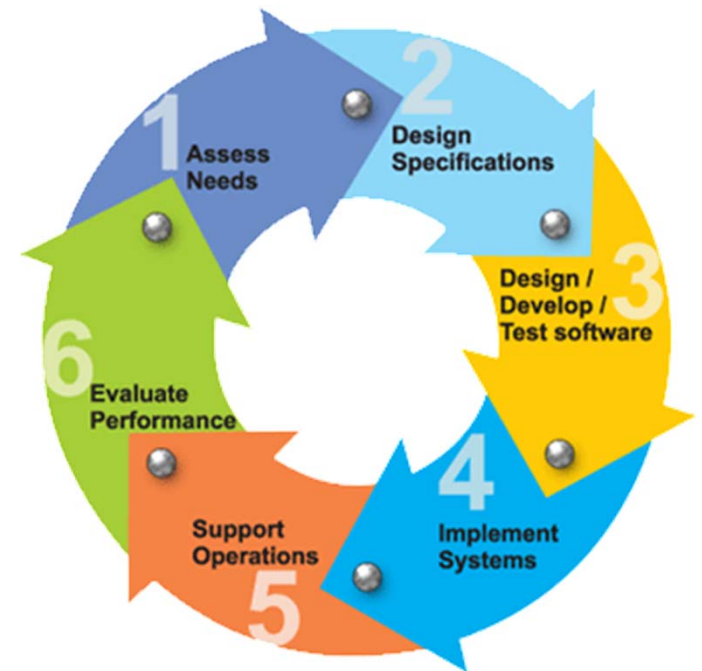
- Security testing of changes (automated/manual)
- Regression testing
- Bug tracking integration



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

<http://cisecurity.org/en-us/?route=downloads.multiform>

http://www.nsa.gov/ia/guidance/security_configuration_guides/current_guides.shtml

- OWASP Backend Security Project

http://www.owasp.org/index.php/Category:OWASP_Backend_Security_Project

- Automated open-source and commercial tools

Standards & checklists

- OWASP Application Security Verification Standard Project

http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

- The OWASP Code Review Top 9

http://www.owasp.org/index.php/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