



The Tangled Web: Web Security 2007

Panelist Slides for Joel Scambray
SecureWorld Expo, Seattle
October 31, 2007





The Web App Threat Environment

- Ubiquity
- Simple to understand (and attack)
- Anonymity
- HTTP/S passes most firewall policies
- Evolving dev models
- Stateless security

What makes the Web fun also makes it challenging to secure.



Moving in the wrong direction?

- Web 2.0 (AJAX, SOAP, etc.)
 - More built-in logic to exploit (Samy worm)
- Convergent, compelling logic (bye-bye static HTML)
 - Mobile, webmail, IM, GIS, social networking, etc.
- Attacking the user experience
 - Phishing, etc.
- More complex dev model
 - Outsourcing, viral frameworks – who's accountable?
- The auditors have noticed
 - PCI DSS 1.1: 11.3.2 . . . and more coming?



Five Things A CISO Should Do

1. Triage: OWASP Top 10 '07 assessment
2. Quantify & justify the investment
 - Focus on how this helps the customer
3. Integrate into dev process, culture
 - (see next)
4. Proactive dev tools & training
 - Managed code, I/O security, session management & crypto
5. Monitor, measure, & improve
 - What stats matter to the business?



Security in the Development Lifecycle

