The Need for Confluence

The Essential Role of Incident Response

in Secure Software Development

OWASP

The OWASP Foundation

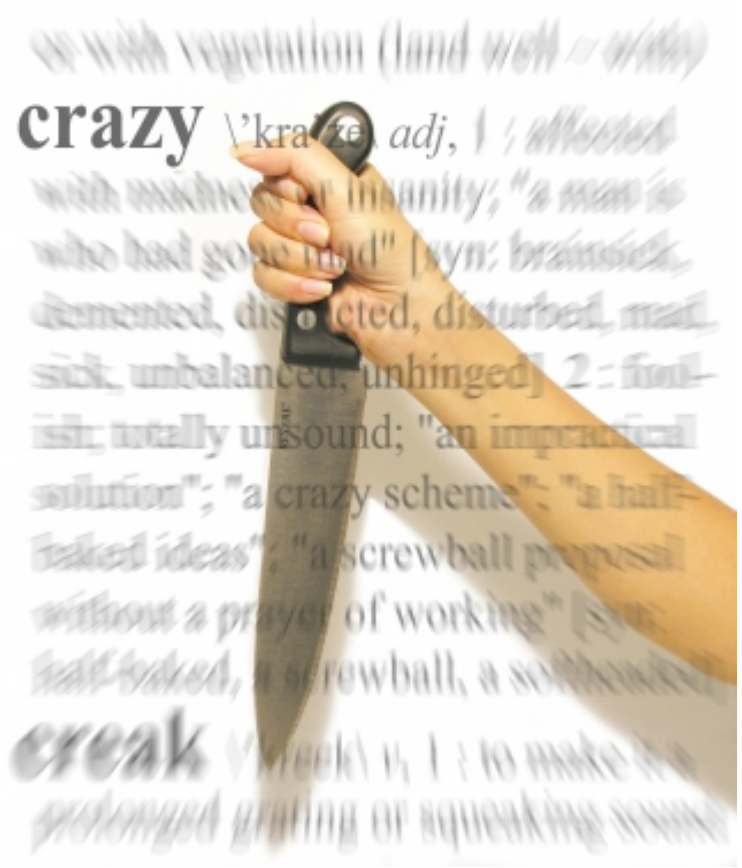
http://www.owasp.org

Why do security incidents occur?

What are the root causes?

What is the definition of insanity?

- Year after year
- Thousands upon thousands of incidents
- Same root cause
- What are we doing about it?
- We talk about proactive, but do we do it? Really?



OWASP

You can't bolt security on later

- A room full of firewalls, intrusion detection|prevention systems, etc., will not protect bad software
- We must address the root causes
- Active participation in development

OWASP

Why aren’t things improving?

OWASP

Learn from history

- We don’t pay enough attention to our failures
- Consider other engineering disciplines

Lack of knowledge

- Developers tend to not have security knowledge
- Security team tends to not have development knowledge
- “Us” and “them”

OWASP

We're overly trusting

- We tend to have misplaced trust in our users
- Sometimes users are malicious
- Sometimes they don't even try to be

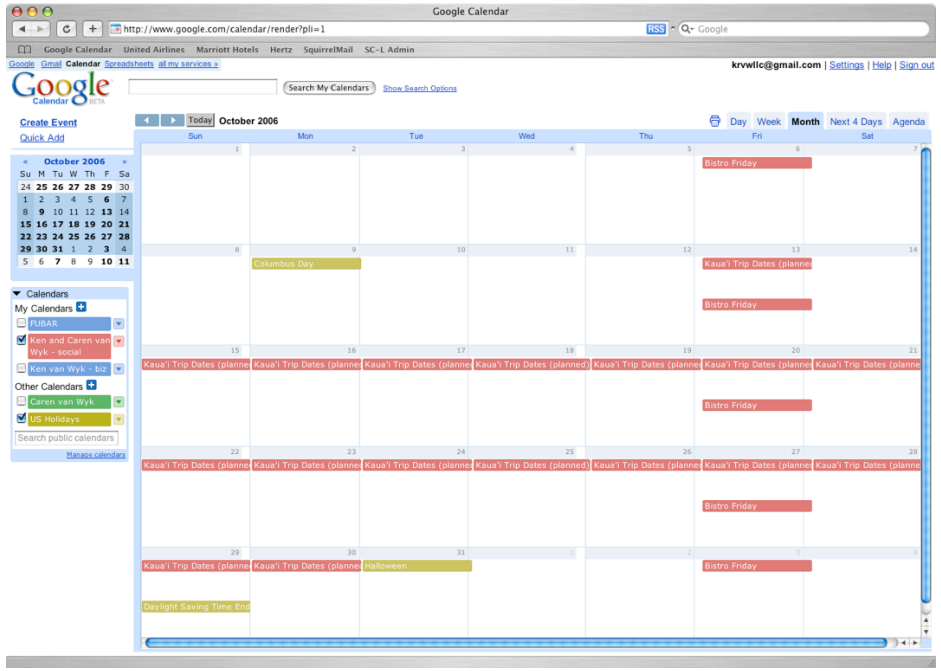
OWASP

Focus

- Too much attention is paid to functional spec
- Consider what can go wrong as well

Complexity

- Complexity is fighting us every step of the way
- Consider AJAX



Connectivity

- Connectivity is everywhere
- Do you know where your data is?
- Consider mobile users, SOAP, grid computing

Extensibility

- Extensibility isn't what it used to be
- Who wants a computer that isn't?
- Is your desktop user privileged?

Old school paradigms

- Old school information security solutions don't adequately protect the software
- Consider IM, Skype, WiFi, VPNs

Testing isn't working

- Software testing does not adequately address security
- Penetration testing is not sufficient

So how can we help?

- Deep integration into the development process
- Consider five stages
  - Requirements
  - Design
  - Code
  - Testing
  - Deployment

OWASP

But first, think positive

- We're too quick to use negative models
  - Anti-virus products
  - Signature-based IDS
  - Vulnerability scanning
- These are not adequate
  - Think positive validation

Part of the team

- Don't just be a reviewer/auditor
  - Adversarial role can be detrimental
- Be a security consultant to dev
  - Each project
  - Guide and assist the dev team

OWASP

Requirements

- Help build security requirements
  - Regulatory compliance
  - Abuse/misuse cases
- Guide discussions on what bad things can happen

Design

- Help conduct design reviews
- Consider available approaches
  - Microsoft's threat modeling
  - Cigital's ARA

Code

- Learn the technologies
- Help build prescriptive language guidance
  - Input validation
  - SQL utilization
  - Authentication
  - Session management

Testing

- Penetration testing alone is not enough
  - Coverage
  - Internals
- Consider Microsoft's testing approach
  - Fuzzing
  - Pen testing
  - Dynamic validation

Deployment

- Verification of safe deployment environment
  - Not just pen testing
  - Host hardening
  - File access controls
  - Event monitoring

Issues to consider

- Cultural barriers
  - Years of “us and them” may be tough to overcome
  - Developers “allergic” to security
  - Authority to mandate
  - Positive incentive

Checklist of things to do

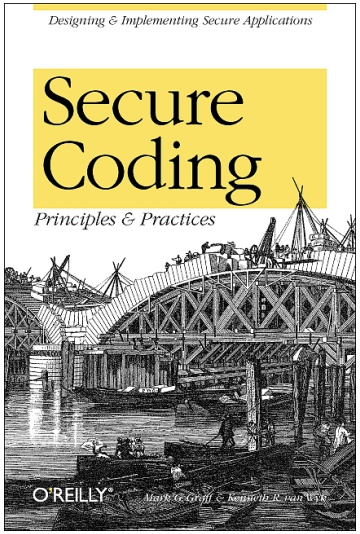
- Read, study, learn
  - Work through OWASP WebGoat exercises
  - Language references
  - See reference list
- Seek dev team
  - Discuss possible roles and responsibilities

Further reading

- The Security Development Lifecycle, Howard and Lipner, Microsoft Press
- Software Security: Building Security In, McGraw, Addison Wesley
- OWASP

Kenneth R. van Wyk
KRvW Associates, LLC

Ken@KRvW.com
http://www.KRvW.com



OWASP