



build | integrate | secure

## Why Do Web Application Vulnerabilities Take So Long to Fix?

**Dan Cornell – Founder and Principal, Denim Group**

**Jeremiah Grossman – Founder and CTO, White Hat Security**

**June 11<sup>th</sup>, 2009**

# Agenda

- Introduction
- How Long Does It Take To Fix Vulnerabilities – Jeremiah Grossman
- Common Reasons Vulnerabilities Are Not Fixed – Dan Cornell
- Questions

## Common Reasons

1. “That Will Never Happen In Production”
2. Our Developers Can’t Fix It
3. Website Will Be Decommissioned “Soon”
4. Solution Conflicts With the Business Use Case
5. Compliance Does Not Require It

## “That Will Never Happen In Production”

- “We have a firewall or IDS that will stop those attacks”
- “No one would ever target *our* site”
- “You would have to be logged in to do that”
- “Only internal users can access that application”
  
- What to Do?
  - *Communicate the true risk*
  - *Promote awareness among developers and managers*

## Our Developers Can't Fix It

- Actually Two Objections: Time and Skills
- Both have scary implications

## Our Developers Can't Fix It: Time

- Fact of Life: **Features > Performance > Security**
- Developers and “The Business” Need to Understand Risk
  - *Compliance requirements*
  - *Brand risk*
  - *Who wants to sign off on not fixing the vulnerabilities?*
- What to Do?
  - *Choose your battles*
  - *Understand that security fixes take time away from new features*

## Our Developers Can't Fix It: Skills

- Even Scariest: How Will This Situation Change Over Time?
- Organizations Won't Be Allowed To Field Vulnerable Applications Indefinitely
  - *Compliance Changes*
  - *Incident Response*
- There Are Many Parts to an Effective Software Security Program
  - *Developers Writing Reasonably Secure Code Is One*
- What to Do?
  - *Work with development managers*
  - *Every developer needs to know something about security*
  - *Some need to know more than others*

## Website Will Be Decommissioned “Soon”

- Example: 10 Year Old Application
  - *To Be Decommissioned “Soon” for Five Years*
- Another Related Issue: No One “Owns” or Understands the Code
- What to Do?
  - *Use mitigating technologies like Web Application Firewalls (WAFs)*
  - *Team with others in the organization who want the application gone*

## Solution Conflicts With The Business Use Case

- Threat Modeling Example:
  - *“Ignoring fraud, what other problems might we run into”*
- Again: **Features > Performance > Security**
- What to Do?
  - *Negotiate based on risk and value*
  - *Compliance requirements can provide a final backstop*

## Compliance Does Not Require It

- Are You Trying To Be “Compliant” Or “Secure”
- What Level of Risk Are You Willing To Accept?
- What to Do?
  - *Leverage compliance as an opportunity to take action*
  - *Don't forget your actual goal is risk management*

## Questions?

Dan Cornell

[dan@denimgroup.com](mailto:dan@denimgroup.com)

Twitter: @danielcornell

Jeremiah Grossman

[jeremiah@whitehatsec.com](mailto:jeremiah@whitehatsec.com)

Twitter: @jeremiahg