

# Defensive Wall 1: Proactive Software Assurance

Andy Prow  
Managing Director,  
Aura Software Security Ltd



# Proactive Software Assurance

“The application layer is now the number one vector for attackers”

- Things you can do to protect your system:
  - Penetration testing
  - Threat Modelling
  - Automated tools and code scanners.
- The idea is “find your security issues before the bad-guys”

# Who are AURA?

- Security Consultants - Penetration Testers
- Founded in 2001
- Performed web application pen-testing for both NZ and international companies.
- Govt, corporate and banking
- Wellington based.

# Are the Threats Real?

- Web-sites allowing us (or a hacker) to:
  - purchase products for free
  - access other user's data
  - access admin features.
  - deny real users access to the system (DOS)
  - access and modify all back-end data.
  - access and modify web-server file-system.
  - create local user AD accounts and then remote admin the machine (via RDP)
  - gain full access to dev-lan and corporate LAN

# Are the Threats Real?

- Desktop / Server applications that allow us to:
  - Monitor usage and activity
  - Insert back-doors allowing full remote access.
  - Weaken encryption algorithms.
  - Gather authentication info (usernames, passwords, hashes)

# Why Attack the App?

- Already tunnelled straight through the firewall – e.g. Web-apps, ports 80 / 443.
- Already authenticated and connected to the DB.
- Already has legitimate access to all the other back-end systems or clients.
- Already performing all the “hacking” tasks we want.

# Defense 1 – Plan for Attack

- Systems
  - How do you know they've been attacked?
  - BCP / DR
- People
  - Who makes the call to "turn it off"?
- Process
  - Incident response and reporting.
  - Staff, contractors, third-parties...



# Defense 2 – Design for Attack

- Threat Modelling
  - Identify all assets to secure
  - Identify and quantify the attacks
- Architecture
  - Critical at both application and enterprise architecture level.
- Framework
  - Design security into all layers of your app framework



# Defense 3 – Secure Dev

- Teach the good guys bad tricks!
  - Train developers in hacking techniques (they love it!)
  - Train testers, project managers, architects etc...
- Pros
  - Your code is more resilient from day 1.
  - Common floors already fixed.
  - Less business logic errors introduced.
- Cons
  - None – do it!



# Defense 4 – Pen-Testing

- Penetration Testing
  - Attempt the common and well-know attacks.
  - Use the tools properly and what the results mean
  - Will attack your more complex “business logic”
- Pros
  - Experts will really try to hack your system.
- Cons
  - Can be expensive!
  - Snapshot in time - can give false security.



# Defense 5 – Automated Tools

- Scanning tools
  - Pen-testing tools
  - Source code scanners
  - Binary scanners
- Pros
  - Repeat scans
  - Can be run without detailed knowledge
- Cons
  - Can be run without detailed knowledge...

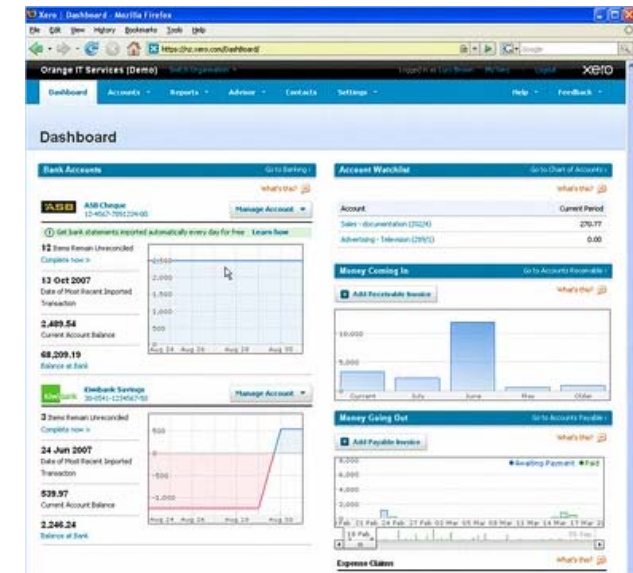


# Most Common Issues?

- Either really good or REALLY bad.
  - Failing to protect against the simplest attacks
  - Running apps and servers with known vulnerabilities.
  - Running apps and servers with admin permissions.
  - No checking
  - No logging
  - Etc...

# Case Study: The Secure Dev

- [www.Xero.com](http://www.Xero.com)
  - Xero – NZ grown online accounting
  - Pen-testing and code review already done
  - Secure developer training (in fact ALL staff – CEO driven!)
  - Devs shown REAL attacks against their code.
  - Devs taught hacking techniques



# Case Study: The Secure Dev

- [www.MyJobCaddy.com](http://www.MyJobCaddy.com)
  - UK based job agency
  - .Net application allowing online CV builder, file upload, admin features etc.
  - Tight “start-up” budget, no time or money for rework
  - One of the few sites we’ve tested with clean pen-test first time!



# The Message

- Most proactive thing can you do is think about the possible security breaches and their real impact.
- Proactively test and RE-test your security before someone else does.
- Teach your good-guys the bad-tricks!

[www.AuraSoftwareSecurity.co.nz](http://www.AuraSoftwareSecurity.co.nz)  
[Andy@AuraSoftwareSecurity.co.nz](mailto:Andy@AuraSoftwareSecurity.co.nz)