Anglia Ruskin University

OWASP
The Open Web Application Security Project

“No GDPR Worries here, I’ve got a Firewall….. the Need for Secure Coding”

Adrian Winckles
Cyber Lead - Anglia Ruskin University
OWASP Cambridge Chapter Leader
Adrian.Winckles@anglia.ac.uk

Anglia Ruskin University

OWASP The Open Web Application Security Project

Bio – Adrian Winckles

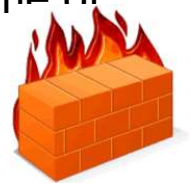
- Director of Cyber Security, Networking & Big Data Research Group and Security Researcher at Anglia Ruskin University.
- OWASP Cambridge Chapter Leader, OWASP Europe Board Member
- Chair for Cambridge Cluster of the UK Cyber Security Forum.
- Vice Chair BCS Cybercrime Forensics SIG
- His security research programs include (in)security of software defined networks/everything (SDN/Sdx), novel network botnet detection techniques within cloud and virtual environments, distributed honeypots for threat intelligence, advanced educational techniques for teaching cybercrime investigation and virtual digital crimescene/incident simulation..

Anglia Ruskin University

OWASP
The Open Web Application Security Project

“No GDPR Worries Here. I’ve got a firewall…..”

- The old adage and corny catchphrase “there are two types of organisation, those who know they’ve been hacked and those that don’t…” still continues to ring true.
- Why do we continue to place our hope in our existing layers and layers of infrastructure protection and our “defence in depth” and if by doing so why are we still suffering breaches and losing our data?
- Those on the dark side only have to be “lucky” once to gain access to your data, we have to be lucky all the time.
- What have we forgotten and what else should we be doing to redress some of the balance to increase our “luck” in the dawn of everything connected to everything else everywhere?



Anglia Ruskin University

OWASP
The Open Web Application Security Project

So if there's lots of infrastructure, I'm safe I've got a firewall….

- Intrusion Detection & Intrusion Prevention
- End Point Protection
- Security Incident Event Management
- VPN
- Anti Virus
- Back end Encryption
- SSL/TLS on everything
- …....

Anglia Ruskin University

OWASP
The Open Web Application Security Project

These are just layers protecting mainly infrastructure…..


Security is like a stack of Swiss cheese
Each slice covers up holes in the slices below it

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Its all about zero days……isn't it?

- Varying different definitions of zero-day attacks
    - attacks on vulnerabilities that have not been patched or made public, while others define them as
    - attacks that take advantage of a security vulnerability on the same day that the vulnerability becomes publicly known (zero-day).
- Generally describes zero-day attacks (or zero-day exploits) as attacks that target publicly known but still unpatched vulnerabilities.
- According to the NSA, "there's no need to blame zero days,. The targets have provided attackers with a wide enough vector through poor cyber hygiene."

Anglia Ruskin University

OWASP
The Open Web Application Security Project

So where are the problems….

- So its not just about the infrastructure layers
- So its not just about protecting the operating system
- So its not just about what's known
- So its not just about what not known (zero days)
- Some of its how we use what we've got (poor cyber hygiene)
- What's left?
  - The Application (s)

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Don’t just take my word for it

Gartner

Anglia Ruskin University

OWASP
The Open Web Application Security Project

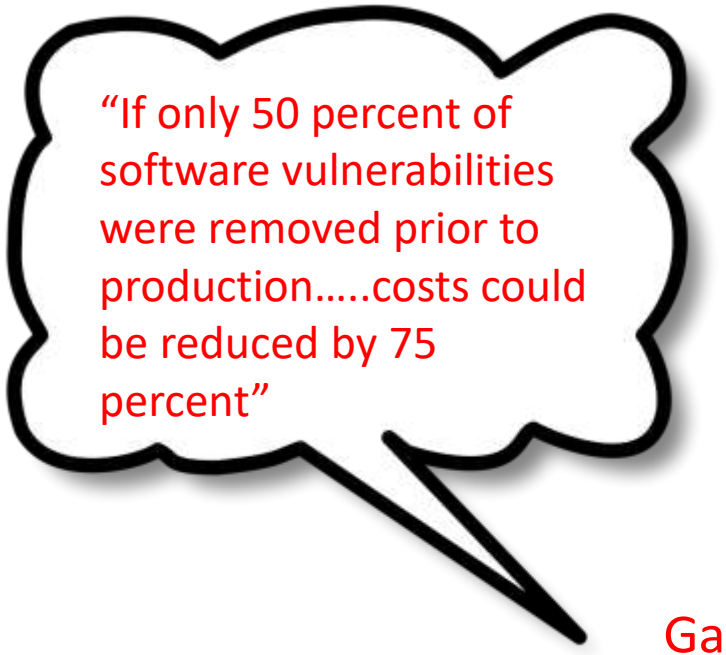
Don’t just take my word for it

Gartner

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Don’t just take my word for it



Gartner

Anglia Ruskin University

OWASP
The Open Web Application Security Project

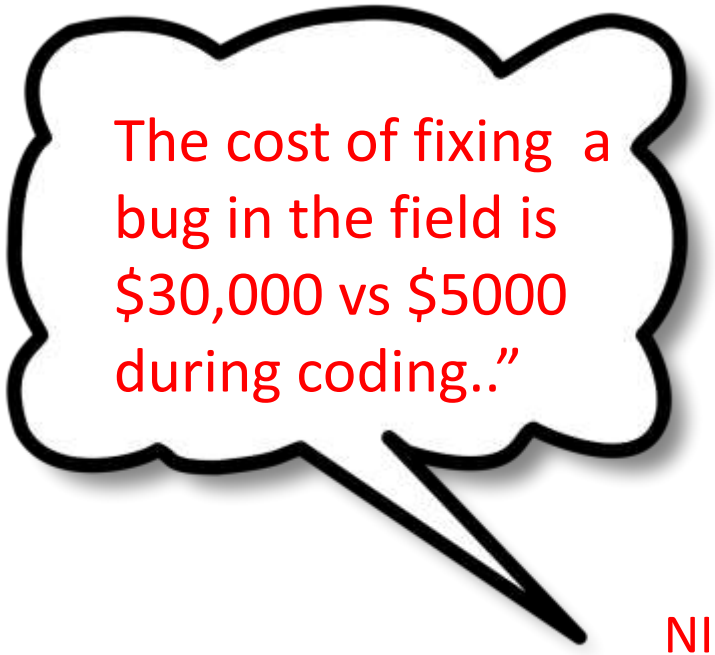
Don’t just take my word for it

NIST

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Don’t just take my word for it

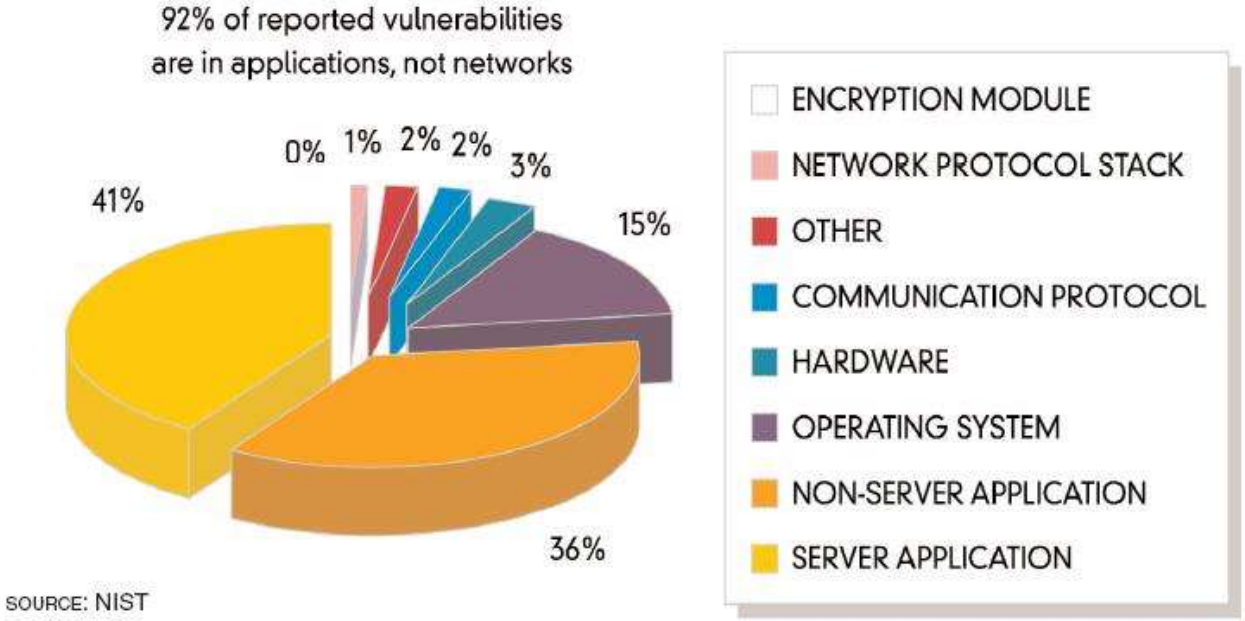


NIST

Anglia Ruskin University

OWASP
The Open Web Application Security Project

How many vulnerabilities are application related?



Anglia Ruskin University

OWASP
The Open Web Application Security Project

If Cars Were Built Like Applications....

- 70% of all cars would be built without following the original designs and blueprints.The other 30% would not have designs.
- Cars would have no airbags, mirrors, seat belts, doors, roll-bars, side-impact bars, or locks, because no-one had asked for them. But they would all have at least six cup holders.
- Not all the components would be bolted together securely and many of them would not be built to tolerate even the slightest abuse.
- Safety tests would assume frontal impact only. Cars would not be roll tested, or tested for stability in emergency maneuvers, brake effectiveness, side impact and resistance to theft.
- Many safety features originally included might be removed before the car was completed, because they might adversely impact performance.
- 70% of all cars would be subject to monthly recalls to add major components left out of the initial production. The other 30% wouldn’t be recalled, because no-one would sue anyway.

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Applications are the big issue….

- Trend is towards the vulnerabilities in the software (could be sensor level, mobile application, hub, cloud back end in the case of IoT) being one of the biggest issues
- Could build the vulnerabilities in by using unsafe libraries or unsafe development environment
- Can be open source or proprietary

webwork Struts

Struts 2

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Sort it with Pentesting?

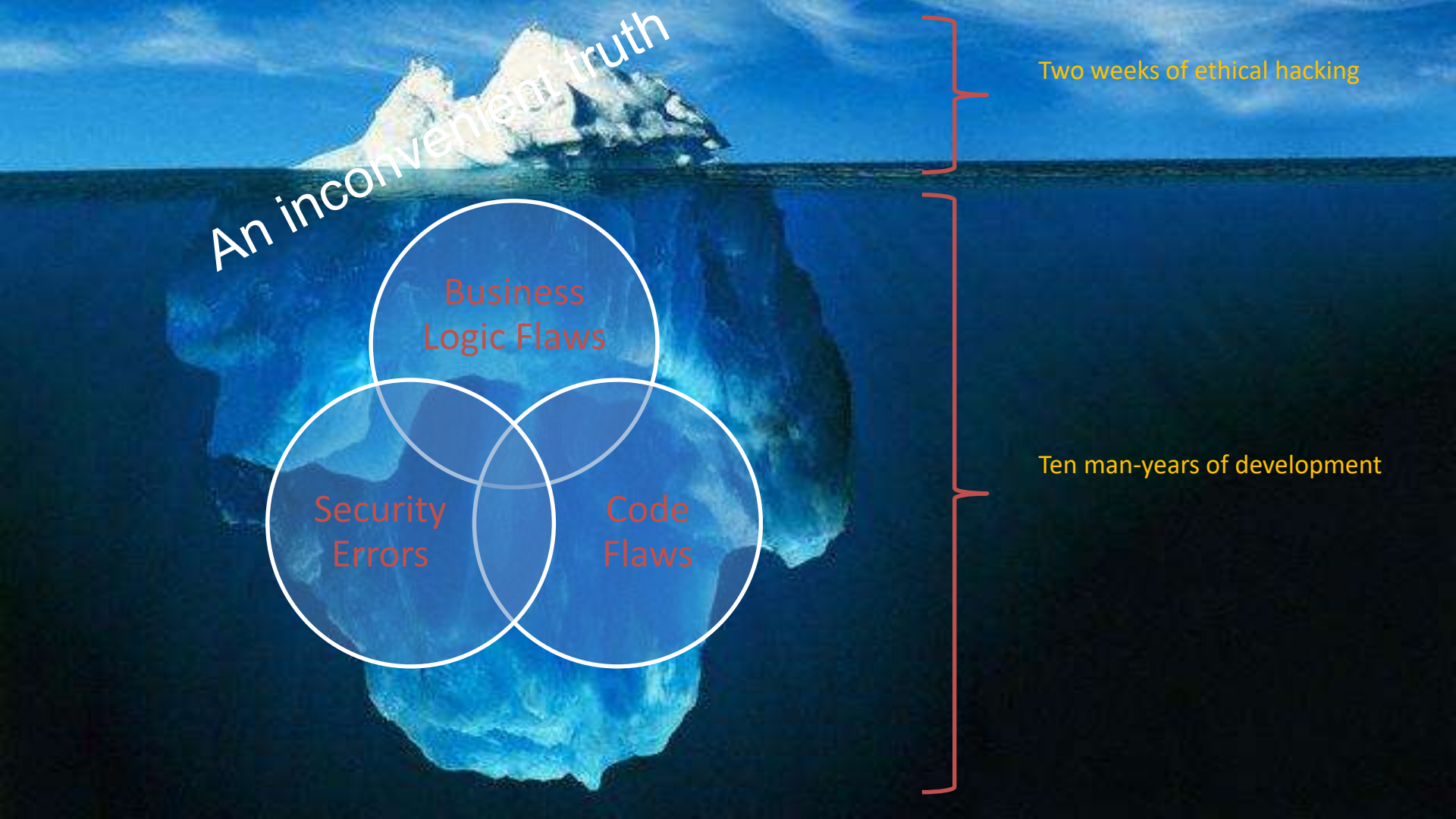
A penetration test is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats.

This is a **component** of an overall security assessment.

- But we are approaching this problem completely wrong and have been for years…..

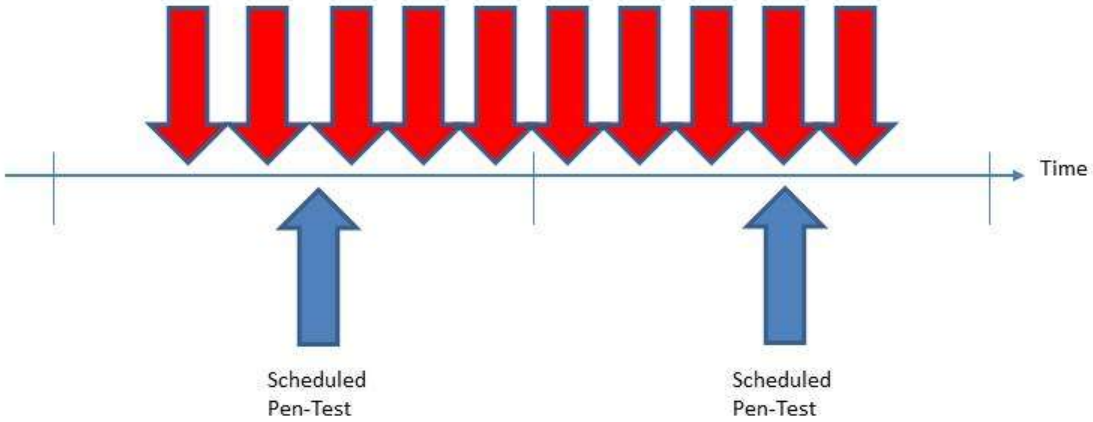
- A traditional end of cycle / Annual pentest only gives minimal security…..

There are too many variables and too little time to ensure "real security".


An inconvenient truth
Business Logic Flaws
Security Errors
Code Flaws
Two weeks of ethical hacking
Ten man-years of development

An Attacker has 24x7x365 to Attack

Attacker Schedule



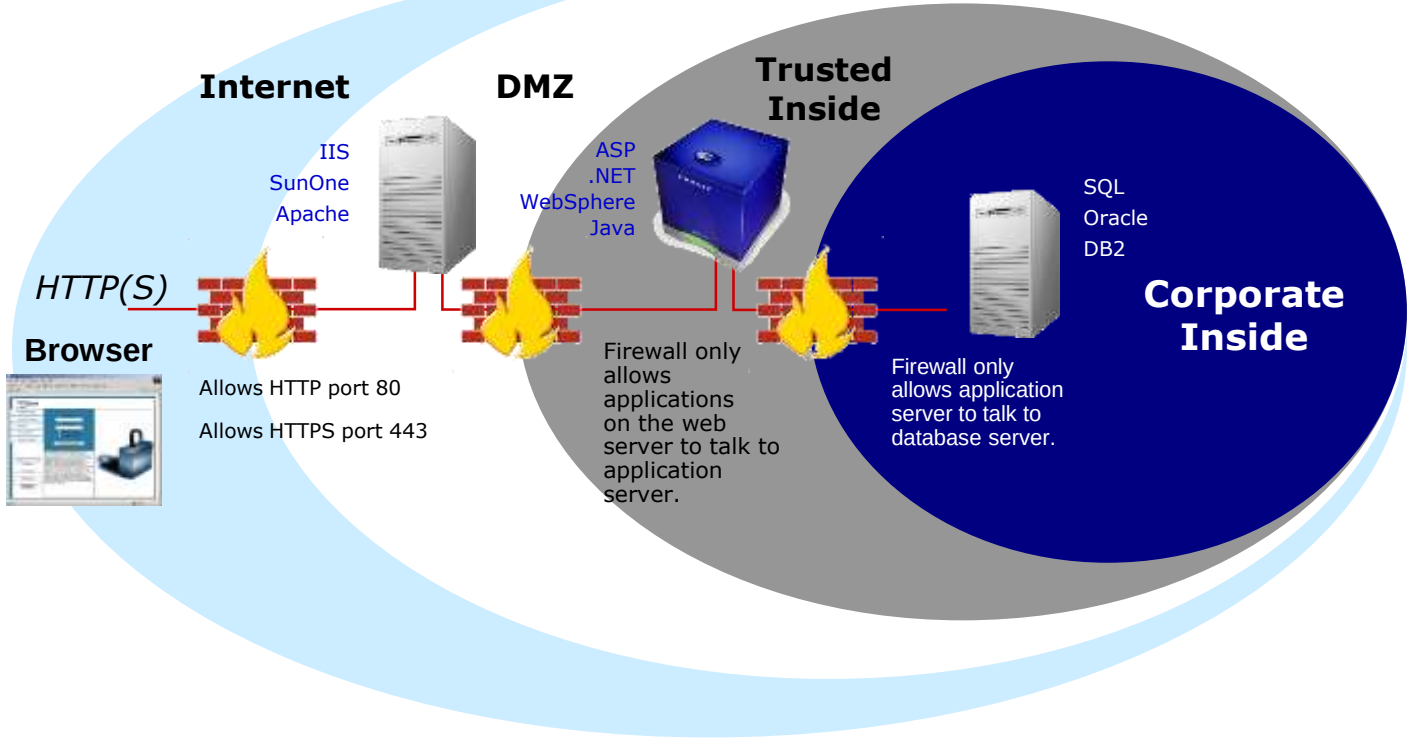
The Defender has 20 man days per year to detect and defend

Who has the edge?

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Web Applications Breach the Perimeter



Anglia Ruskin University

OWASP
The Open Web Application Security Project

Why Application Vulnerabilities Occur

Security Professionals Don't Know The Applications

"As a Network Security Professional, I don't know how my companies web applications are supposed to work so I deploy a protective solution…but don't know if it's protecting what it's supposed to."

The Web Application Security Gap

Application Developers and QA Professionals Don't Know Security

"As an Application Developer, I can build great features and functions while meeting deadlines, but I don't know how to develop my web application with security as a feature."

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Application Vulnerabilities

“If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.”

-Weinberg's Second Law

How do we do fix the problem?

- Security Analyst
  - Understand the data and information held in the application
  - Understand the types of users is half the battle
  - Involve an analyst starting with the design phase
- Developer
  - Embrace secure application development
  - Bake security into frameworks when you can
  - Quality is not just “Does it work”
  - Security is a measure of quality also

How do we fix the problem? (Cont'd)

- QA:
  - Security vulnerabilities are to be considered bugs, the same way as a functional bug, and tracked in the same manner.

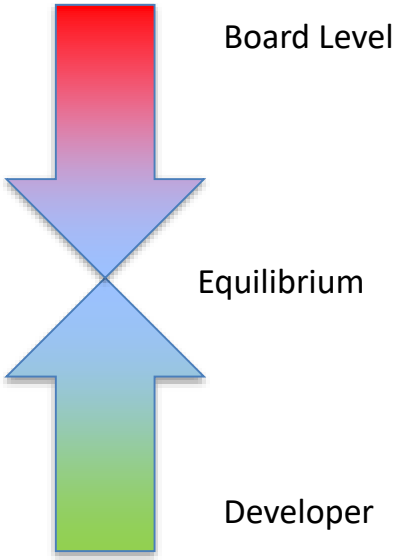
- Managers:
  - Factor some time into the project plan for security.
  - Consider security as added value in an application. – $1 spent up front saves $10 during development and $100 after release

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Bottom Up Problems

- Issues
  - Developers don't have time to test adequately (if at all)
  - Developers don't know secure coding practices
  - Pressure to be first to market,
  - Using untested (COTS) components or libraries (saving time and money)

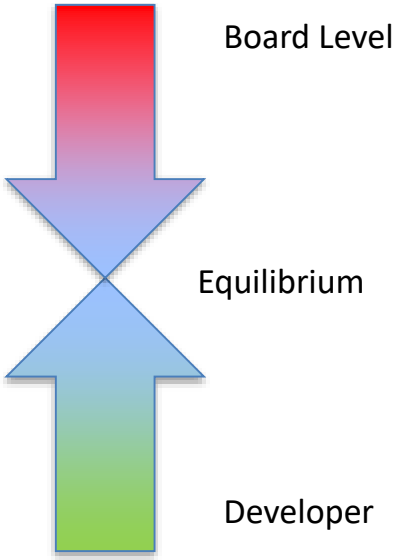


Anglia Ruskin University

OWASP The Open Web Application Security Project

Bottom Up Solutions

- Education
  - Developers taught secure coding techniques
- Testing
  - Not just functionality or user experience but security built in from first principles
  - Sanitise third party products and libraries
  - Testing throughout SDLC
  - White box, not just last minute black box pen testing

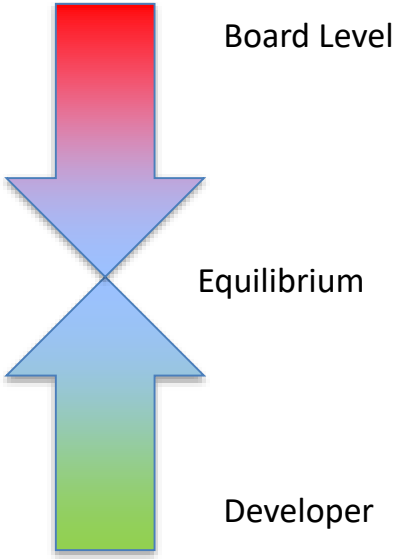


Anglia Ruskin University

OWASP
The Open Web Application Security Project

Top Down Problems

- Issues
  - Pressure to be first to market, focus on product features and user experience, **NOT** Security.
  - Cost reduction ignoring security risk
  - Security not seen as a Boardroom priority
  - Lack of a security culture

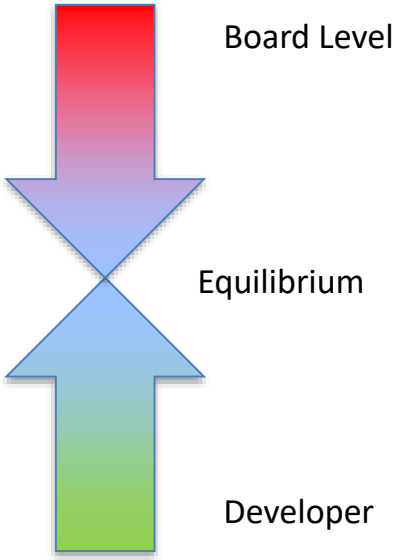


Anglia Ruskin University

OWASP
The Open Web Application Security Project

Top Down Solutions

- Education
  - Boardroom & Senior management necessity to build security in from the start.
- Representation
  - Appoint a CISO to the Board.
  - Develop a Security Culture



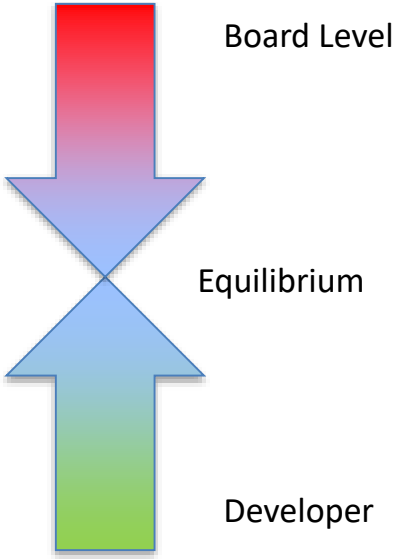
Anglia Ruskin University

OWASP
The Open Web Application Security Project

Top Down vs Bottom Up Solutions

- Equilibrium is needed
- Most Important

BUILD SECURITY IN!!



Anglia Ruskin University

OWASP The Open Web Application Security Project

Need for Education

- Educate Users
  - Security Awareness Programs – Everyone's responsibility
- Educate Developers – Secure Coding (Under-16/FE/HE)
  - Next generation embed into computer science curriculum's
    - CPHC/BCS/ISC2 Communities of Practice Initiative
    - OWASP Application Security Framework Curriculum
    - New IISP/CREST Academic Framework
  - Existing Generation
    - Secure Coding Programs and Workshops and Revision Follow-up's (a dog's not just for Christmas)

Anglia Ruskin University

OWASP The Open Web Application Security Project

Need for Education (Cont'd)

- QA:
  - Testing throughout the SDLC – not just at the end
  - OWASP Testing Guide
- Board
  - Educate Board members to build security in from the start as a business benefit
  - Security is everyone's responsibility

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Who can help?

Anglia Ruskin University

OWASP
The Open Web Application Security Project

OWASP – The Open Web Application Security Project

- The Open Web Application Security Project (OWASP) is a not-for-profit group that helps organizations develop, purchase, and maintain software applications that can be trusted.
- OWASP educates developers, designers, architects and business owners about the risks associated with the most common Web application security vulnerabilities.
- The organisation's most well known "product" is the popular Top Ten list that explains the most dangerous Web application security flaws and provides recommendations for dealing with those flaws.
- OWASP supports and sponsors tools, document and code library projects
  - Tools and documents that can be used to find security-related design and implementation flaws, tools and documents that can be used to guard against security-related design and implementation flaws and
  - Code Libraries that can be used to add security-related activities into the

Ang
Uni

Security Project

A QUICK DEVELOPER'S GUIDE

TO OWASP PROJECTS

Learn how to secure your web applications against the most common web vulnerabilities

OWASP

2015

I'm new to application security...where should I start?

#1

We strongly recommend you to look at some quick guidelines such as:

Watch the APPSEC tutorial series to get you started

OWASP TOP TEN: the classic guidelines

OWASP Cheat Sheets to get into the stuff without getting annoyed

I want to 'see' vulnerabilities and learn how they happen...

#2

We have some cool 'vulnerable applications' to learn how you should not code them:

Security Shepherd: Great app for understanding vulnerable web apps including lessons

WebGoat: OWASP classic JAVA vulnerable site with lessons, all solutions can be found in Youtube videos

OWASP Bricks: A PHP vulnerable site with lessons

I want to use pen testing tools to 'hack' my apps and test for vulnerabilities

#3

If you wan to get into pen testing, some cool tools will help you to learn more about it and they can assist you with testing your website

OWASP ZAP: an attack proxy , creme de la creme tool for hacking your site

OWTF: A complete pen testing framework which includes test cases and it's aligned with the latest security standards

Xenotix Exploit: Indulge into XSS with this tool

#4

1
2
3

Is there a checklist to make sure I don't forget anything?

OWASP ASVS is 'the list' you can apply to your development process. The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security control

The Secure Coding Practices Quick Reference Guide is a technology agnostic set of general software security coding practices, in a comprehensive checklist format, that can be integrated into the development lifecycle. At only 17 pages long, it is easy to read and digest.

#5

LIB
LIB

OK. Is time to secure my site!

If you are looking for specific code libraries to protect your application against some nasty vulnerabilities and attacks, here are some great ones:

Appensor: Intrusion detection for your site

OWASP HTML Sanitizer is written in Java which lets you include HTML authored by third-parties in your web application while protecting against XSS

CRSFGuard: Protect your site against CRSF attacks

#6

How can I check for vulnerable libraries in my application?

Keeping up to date with the latest vulnerabilities is not easy, let alone finding them in your dependency libraries. What about a tool that helps you check this automatically ?

Dependency-Check is a utility that identifies project dependencies and checks if there are any known, publicly disclosed, vulnerabilities. Currently Java, .NET, and Python dependencies are supported. This tool can be part of a solution to the OWASP Top 10 2013

#7

COOK BOOK

What about a Developer's Guidelines?

The OWASP Developer Guide is the original OWASP project. It was first published in 2002, when Ajax was only a mote in Microsoft's eye with the new e-mail notification in Outlook Web Access (and only if you used Internet Explorer). Since then, the web has come a long way.

#8

I want to analyse my code deeper...

OWASP has also Guidelines and Static Analysis tools like:

Code Review Guidelines: How to check and review your code for common vulnerabilities

O2 Platform : Strong Static Analysis tool which can also be a very powerful prototyping and fast-development tool for .NET.

Check more projects

Visit OWASP projects wiki page to learn more about application security :
https://www.owasp.org/index.php/Category:OWASP_Project#tab=Project_Inventory

Anglia Ruskin University

OWASP
The Open Web Application Security Project

Questions?