



Mark curphey @curphey

COMMUNITY "THE KILLER APP" at OWASP APP SEC USA













Saturday, September 24, 11



Saturday, September 24, 11



=



2001

2011

Family



← Started OWASP

Work

/ Internet
Security
Systems

/ Charles Schwab

/ Watchfire

/ Foundstone

/

/

Microsoft

Living

Atlanta

San Francisco

Boston

France

UK

Seattle

2001

2011

3/02/2003 – Space Shuttle Disintegrates

24/10/2002 – Snipers in DC

9/11/2001 – Twin Towers

04/11/2008 – President Obama, first black president

10/03/2003 – Bombing Starts in Iraq

29/08/2005 – Hurricane Katrina

26/12/2004 – Indonesia Tsunami

29/09/2008 – Dow falls 788 points

2011 – Arab Spring

2001

2011

07/2004 - Ruby on Rails released

15/01/2001 - Wikipedia Launched

2003 - First Web 2.0 conference

23/10/2001 - iPod unveiled

08/2/2005 - Term Ajax coined by Jesse James Garret

23/04/2005 - First video uploaded to YouTube

2/2004 - FaceBook created

3/2009 - FourSquare launched at SXSW

26/3/2006 - Twitter created

02/10/2008 - Chrome Browser released

09/01/2007 - iPhone unveiled

2001 - 0.5 billion with internet access

2011 ~2 billion with internet access

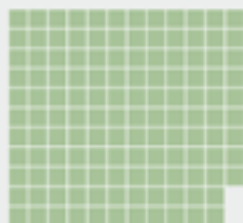
2001

2011

■ = 1 million records lost, colored by breach type (hack, stolen, lost, or fraud)

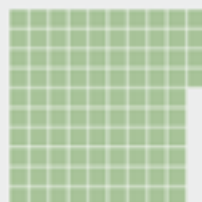
Heartland Payment Systems

130m records lost – Hacked
January 20, 2009



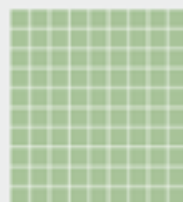
TJX Companies, Inc.

94m – Hacked
January 17, 2007



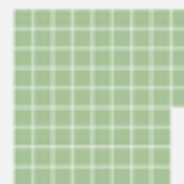
TRW

90m – Hacked
June 1, 1984



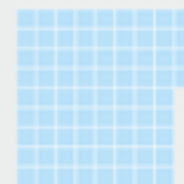
Sony Corporation

77m – Hacked
April 26, 2011



National Archives and
Records Administration

76m – Improper disposal
October 5, 2009



CardSystems

40m – Hacked
June 19, 2005



RockYou, Inc.

32m – Hacked
Dec. 14, 2009



US Dept. of
Veterans Affairs

26m – Stolen
May 22, 2006



HM Revenue
and Customs

25m – Lost
Nov. 20, 2007



Sony
Corporation

25m – Hacked
May 2, 2011



T-Mobile

17m – Lost
Oct. 6, 2008



Canada
Revenue Agency

16m – Stolen
Nov. 1, 1986



Bank of New
York

12m – Lost
Sept. 6, 2008



GS Caltex

11m – Lost
Sept. 6, 2008



Dai Nippon
Printing Company

9m – Fraud
March 12, 2007



Fidelity National
Info. Services

8m – Fraud
July 3, 2007



TD Ameritrade

6m – Hacked
Sept. 14, 2007



Chilean Ministry
of Education

6m – Hacked
May 11, 2008



Data Processors
International

5m – Hacked
Dec. 8, 2008



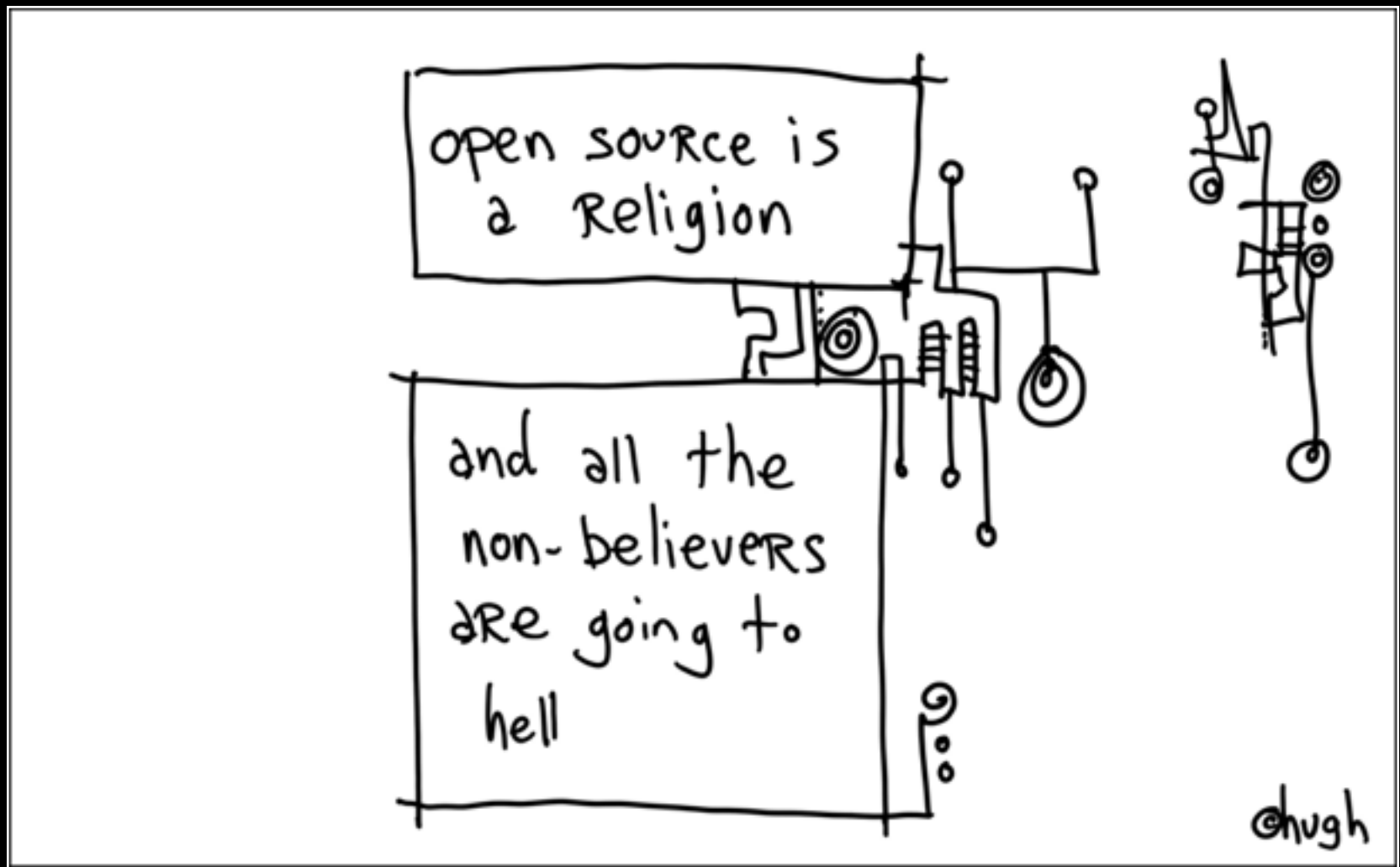
NATHAN YAU, <http://flowingdata.com>




How will OWASP be even better in 2021 ?

(The Hit List | The Watch List | The Wish List)

The Hit List



Open Source (FOSS) as a Model for Trusted Participation

A close-up photograph of a white ceramic mug. The word "coffee" is printed in a black, lowercase, monospaced font on the front of the mug. A white tea bag string hangs over the left rim of the mug, with the tea bag itself resting on the surface in front of the mug. The background is blurred, showing a light-colored surface and some indistinct shapes.

coffee

1. No Golden Rules
2. Rules Don't Seem to Help



Communities are Like Gardens

Community Tools Matter





Data



Information



Presentation



Knowledge

There Are Recipes for Project Success

It's Not What You Say You Are Going To Do, But
What You Actually Do That's Important





**YOU DON'T NEED
AN ORGANIZATION
TO BE ORGANIZED**

Connecting People In Person Together is Critical



OWASP Spain Chapter Meeting – May 2009, Madrid



OWASP

The Open Web Application Security Project



Like-Minded People Connect



OWASP Charity Run

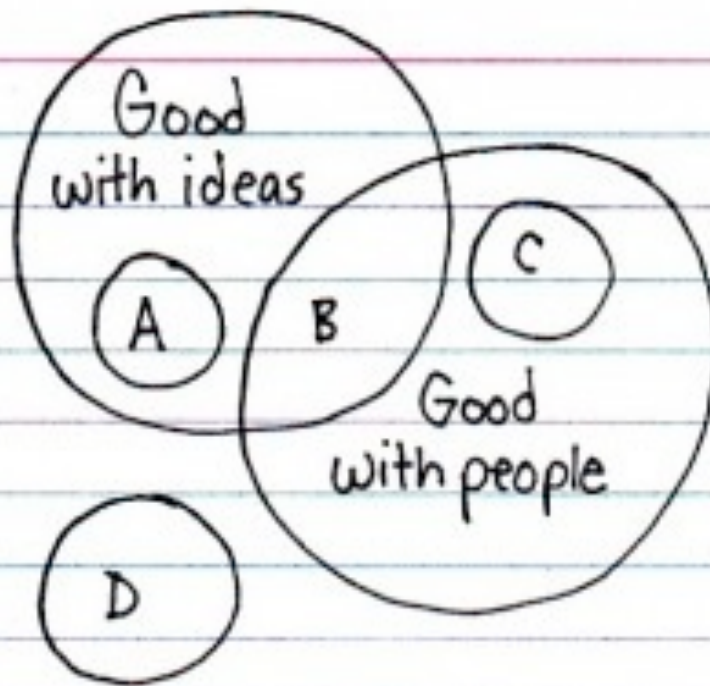
80% of the effects come
from 20% of the causes

“Pareto Principle”





The Cream Always Rises to
the Top



A = Prima donna

B = Savior

C = Pushover

D = Nightmare



Communities are Organic

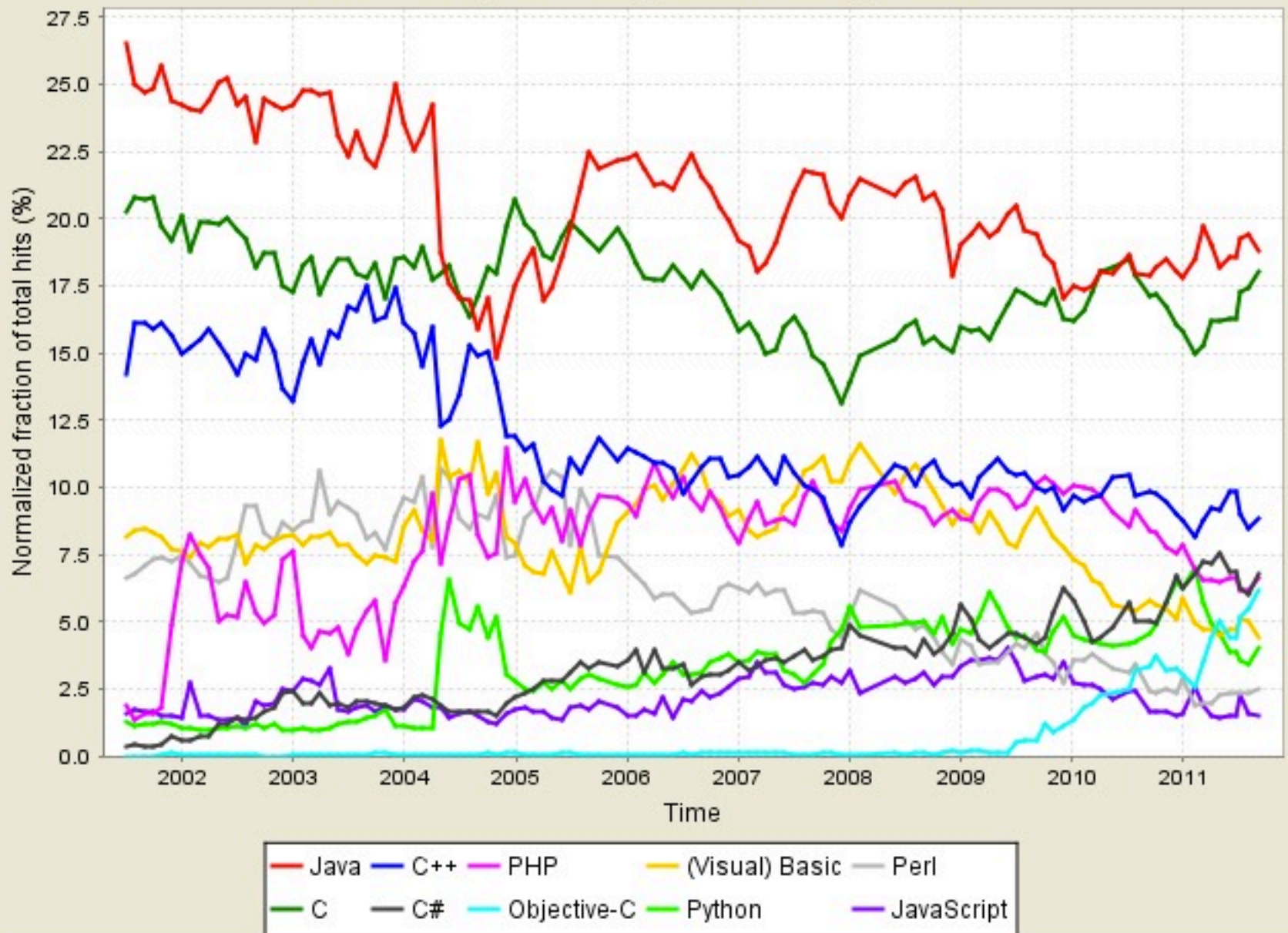
It Doesn't Matter How Fast You Are Running If
You Are Moving In The Wrong Direction



Personal Recognition of Some Exceptional People

The Watch List

Tiobe Programming Community Index



What Are the Hipsters Building With ?

Test Driven Development

Continuous Integration & Delivery

Big Data & Map Reduce

Behaviour Driven Development

JQuery

Node.js

HTML5 + CSS3 + JavaScript

Agile

Django

NoSQL

JSON

CoffeScript

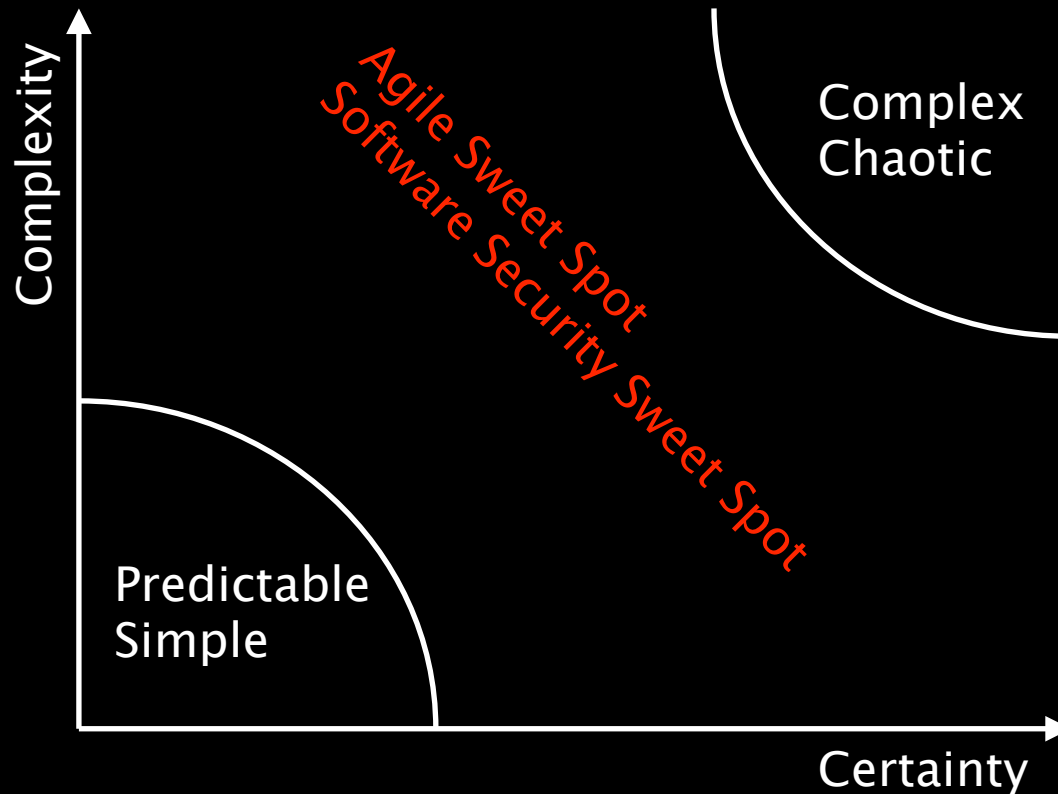
Rails

Clojure

oAuth 2.0

FB Connect

Embracing Agile



“The Ralph Stacey Diagram”

Security People

Developers

Operations

As seen by
Security People



As seen by
Developers



As seen by
Operations



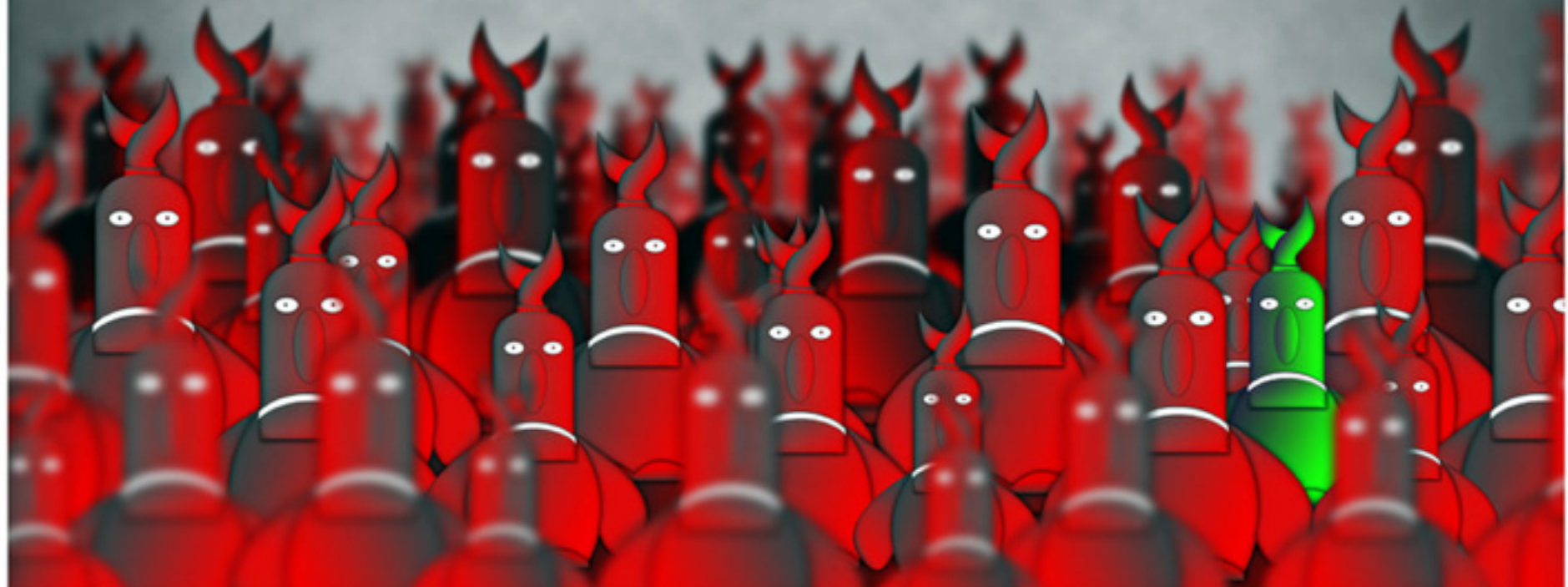


Everyones Unique



Being Unique Is Generally
Not A Good Thing

When You Are The Odd One Out It's Tough to Influence



For Most Developers



Security < Performance < Features

So OWASP Must Be As Easy As
Ordering a Sandwich

1. Choose Your Bread
2. Choose Your Fillings
3. Your Choose Toppings
4. Eat Your Sandwich

1. Choose Your Frameworks
2. Choose Your Languages
3. Choose Your Scenarios
4. Get Your Knowledge & Tools



Builders

Developers
Architects

Breakers

QA / Testers
+ Security Testers

Defenders

Operations

It's Time to Move on From A
Vulnerability Centric Project View

The Wish List

My Wish List for OWASP 2011 to 2021

ALL About People



1. It has a CFO - Chief Finance Officer
(better funding & partnerships)
2. It has a CTO - Chief Technology Officer
(product & engineering management)
3. It has a CKO - Chief Knowledge Officer
4. It has a Head Teacher (CEO title didn't work!)
5. It has a CPO - Chief People Officer
(make life great for volunteers)
6. It has a 'hack house'
(free lodging + food in a nice place for
volunteers & interns)

OWASP Security Tools for Developers Project

Mini-summit / kick-off tonight
(Probably in a bar somewhere)

All welcome (really good Java
developers welcome even more
than all) ;-)

@curphey on Twitter this
afternoon #owasp

mark@curphey.com | @curphey



That's All Folks!