relevance

Auditing Code: Taking a Look at Taking a Look

Aaron Bedra

Central Ohio Information Security Summit

May 8, 2009

Background

Agenda

Establishing a Baseline

Setting Expectations

Where to Look

Tricks to Maximize Effectiveness

When Enough is Enough

How to Deliver Results

relevance

Establishing a Baseline

Who, What, Where, When, How


relevance


relevance

Who

What

Where

When

How

relevance

Setting Expectations

Deliverables, Legal Requirements, Stopping Points

Deliverables

Legal Requirements

Stopping Points

Now is a good time to sign the paperwork

relevance

Where to Look

People, Places, and Things

People

Places

Things

relevance

Maximizing Effectiveness

Automated Tools, Static Analysis, Manual Follow-up

Automate Everything!

Static Analysis

Manual Follow-up

relevance

Enough Already

When it's time to call it

All goals have been achieved

A major, earthshatering vulnerability has been found

Testing window is closed

You couldn't find anything


Y
d

relevance

Delivering Results

How to break it down

Pro Tip:
Your job is **only** to report the facts!

Make short, concise statements about the issues

When possible, link to detailed explanations

relevance

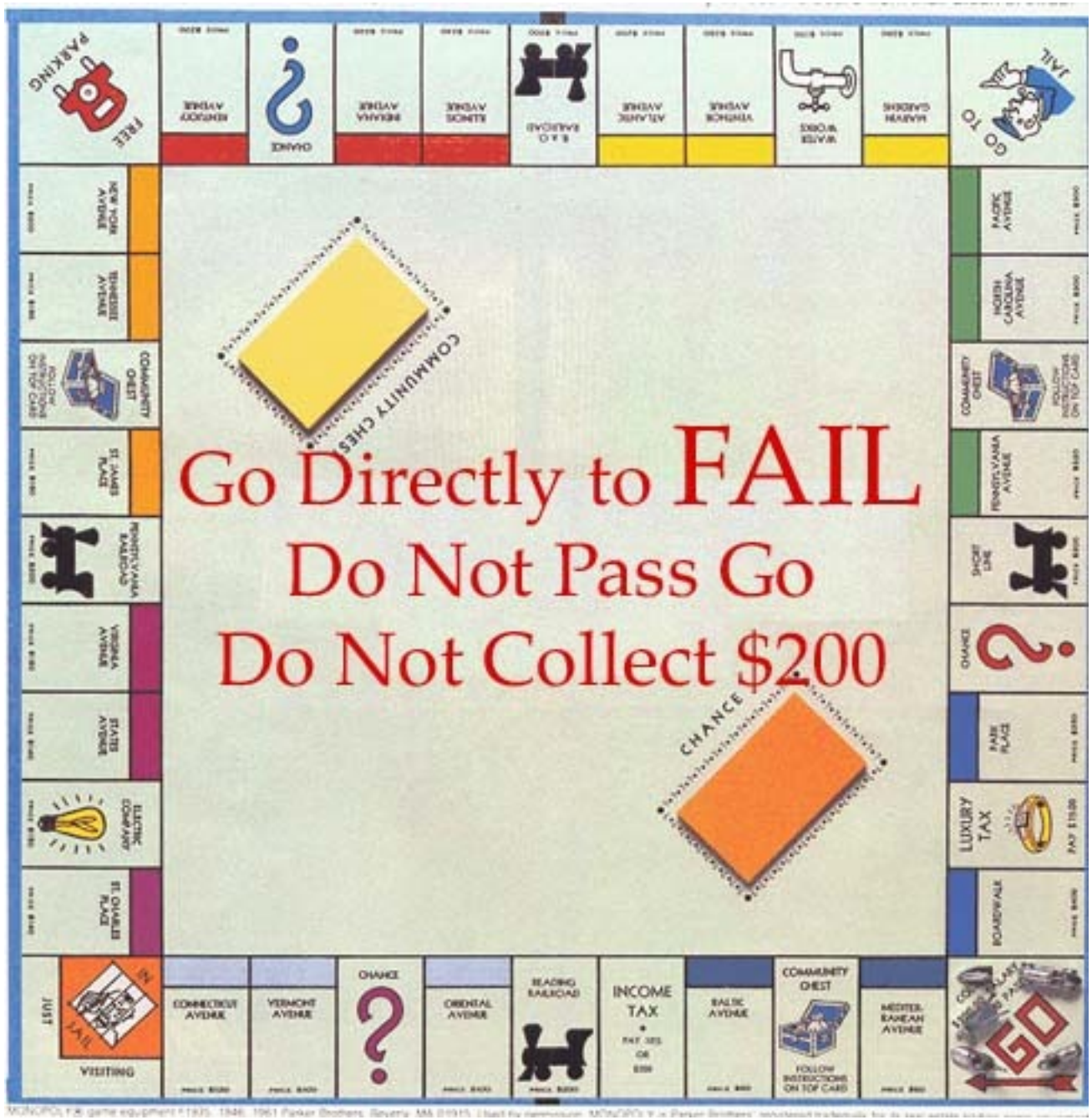
A Tale of Fail Most Epic

Meet Joe

Joe is having a bad day

Meet Michael

relevance


Go Directly to FAIL
Do Not Pass Go
Do Not Collect $200
COMMUNITY CHEST
CHANCE
GO
JAIL
FREE PARKING
INCOME TAX
LUXURY TAX
READING RAILROAD
B. & O. RAILROAD
PENNSYLVANIA RAILROAD
SHORT LINE
VISITING
JUST IN JAIL

None of is as dumb as all of us

DEMO

Resources

- github.com/abedra/presentations/auditing-code
- github.com/abedra/safe-erb
- github.com/relevance/tarantula
- www.owasp.org/index.php/Top_10_2007
- www.infoq.com/presentations/secure-programming-static-analysis

relevance

Discussion and Questions