Why can’t we build secure software?

Tanya Janca
Security Trainer and Coach at SheHacksPurple.dev

@SheHacksPurple
HOW DO I FIX THIS SECURITY BUG?

YOU SHOULD KNOW!
Why can’t we build secure software?
The mandatory “about me” slide.

AKA: @SheHacksPurple

I’m Tanya Janca.

Security Trainer at SheHacksPurple.dev
Let’s do this!
THE DEVELOPERS DIDN'T IMPLEMENT ANY SECURITY FIXES

THEY SAID THEY'LL FIX THEM IN THE NEXT RELEASE.
DEVELOPER

AFTER THE SECURITY REPORT
All of this creates the feeling of insecurity about people’s jobs and how to do them well.

Which leads to predictably negative behaviour...
Deviant Behaviour
Moral Disengagement
Reduced Job Involvement
Risk Taking Behavior
Reduction of Organizational Citizenship Behavior

(positive workplace activity and involvement)
All of this negative behavior leads to insecure software.

Hypothesis
IT'S TIME FOR SOLUTIONS!
The Plan:

1. Support dev and sec team with processes, training, and resources so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with *processes*, training, and resources so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with processes, **training**, and resources so they can confidently get the job done.
2. Initiate and then maintain culture change.
The Plan:
1. Support dev and sec team with processes, training, and **resources** so they can confidently get the job done.
2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with processes, training, and resources so they can **confidently** get the job done.

2. Initiate and then maintain culture change.
The Plan:
1. Support dev and sec team with processes, training, and resources so they can confidently get the job done.
2. Initiate and then maintain culture change.
PROCESSES
YOU DON'T HAVE AN APP SEC TEAM?
YOU WANT TO "MATRIX" ME INTO THE PROJECT TEAM?
Start Security Earlier!

Push Left!
Break security activities into smaller pieces
I DON'T ALWAYS VALIDATE MY VA RESULTS

BUT WHEN I DO, I DO IT IN PRODUCTION
YOU DON'T HAVE TO KNOW EVERYTHING
SECURITY LESSONS FOR EVERYONE!
Provide free training to developers

Photo: DevOpsDays Zurich, May 2018, with Nicole Becher of OWASP DevSlop
PROVIDE FREE SECURITY TRAINING

OFTEN

DON'T STOP!
(Off Colour) Job Shadowing
RESOURCES
WEB APP SECURITY STANDARDS!
I TRIED TO READ THE SECURITY STANDARD
THEY'LL NEVER FIND THE NEW SECURITY STANDARD
Give Developers Security Tools!
(They just might use them)
UHHHH, WHO'S PAYING?
OWASP: Your new BFF!!!

The Open Web Application Security Project
NO MORE BLAMING
WE ALL MAKE MISTAKES

NO NEED TO RUB MY NOSE IN IT
ROOMMATES

SEC AND DEV!
WE'RE SCREWED

A message for conferences

No more “we’re screwed” keynotes.
BE A TRUE LEADER

Lead By Example
Conclusion

<the plan>
The Plan:

1. Support dev and sec team with processes, training, and resources so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with **processes**, training, and resources so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with processes, **training**, and resources so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:

1. Support dev and sec team with processes, training, and **resources** so they can confidently get the job done.

2. Initiate and then maintain culture change.
The Plan:
1. Support dev and sec team with processes, training, and resources so they can **confidently** get the job done.
2. Initiate and then maintain culture change.
The Plan:
1. Support dev and sec team with processes, training, and resources so they can confidently get the job done.
2. Initiate and then maintain culture change.
Call To Action

It has to start somewhere...

Why not with you?
Conclusion

</plan>
Resources: Open Web Application Security Project

#OWASPLove

https://owasp.org

meetup.com/OWASP-Victoria-Chapter/
Women of Security welcomes you!

WoSEC

Paris, Ottawa, San Francisco, Singapore, Dallas, Houston, Austin, Vancouver, Portland, Ottawa, Chicago, Bangalore, Boise, Montréal, Zurich, Nairobi, Johannesburg, Stockholm, Victoria, Milwaukee, Detroit, Denver, Barcelona, Madrid

Canada, France, USA, India, Switzerland, Kenya, South Africa, Sweden, Spain

@WoSECntweets
Resources: ME!

Follow me?

SheHacksPurple.dev

Twitter: @SheHacksPurple

https://medium.com/@SheHacksPurple
https://dev.to/SheHacksPurple
https://YouTube.com/SheHacksPurple
Thank You

Tanya Janca
Tanya@SheHacksPurple.dev
Security Training and Coaching
SheHacksPurple.dev