Pushing Left, Like a Boss

Application Security Foundations

OWASP

The Open Web Application Security Project

Tanya Janca

Tanya.Janca@owasp.org

OWASP Ottawa Chapter Leader

OWASP DevSlop Project Leader

@sheHacksPurple

OWASP
The Open Web Application Security Project

What is 'Pushing Left'?

If you imagine the SDLC written out on a piece of paper, the further left you go means the earlier you are in the SDLC process.

“Pushing Left” means security wants to be invited to the party earlier. And for AppSec, this means during the development phase.

OWASP
The Open Web Application Security Project

Who am I?

I'm Tanya Janca; Application security evangelist, web application penetration tester and vulnerability assessor, trainer, public speaker, ethical hacker, OWASP Ottawa chapter leader, OWASP DevSlop project leader, effective altruist, software developer since the late 90's.

I have been paid to be geeky for over 20 years!

I want software to be more secure so that I can use the internet safely. Seriously.

The current state: Everyone is “getting hacked”

YOU HAVE BEEN
HACKED !

The current state: We looking the wrong way.

OWASP
The Open Web Application Security Project

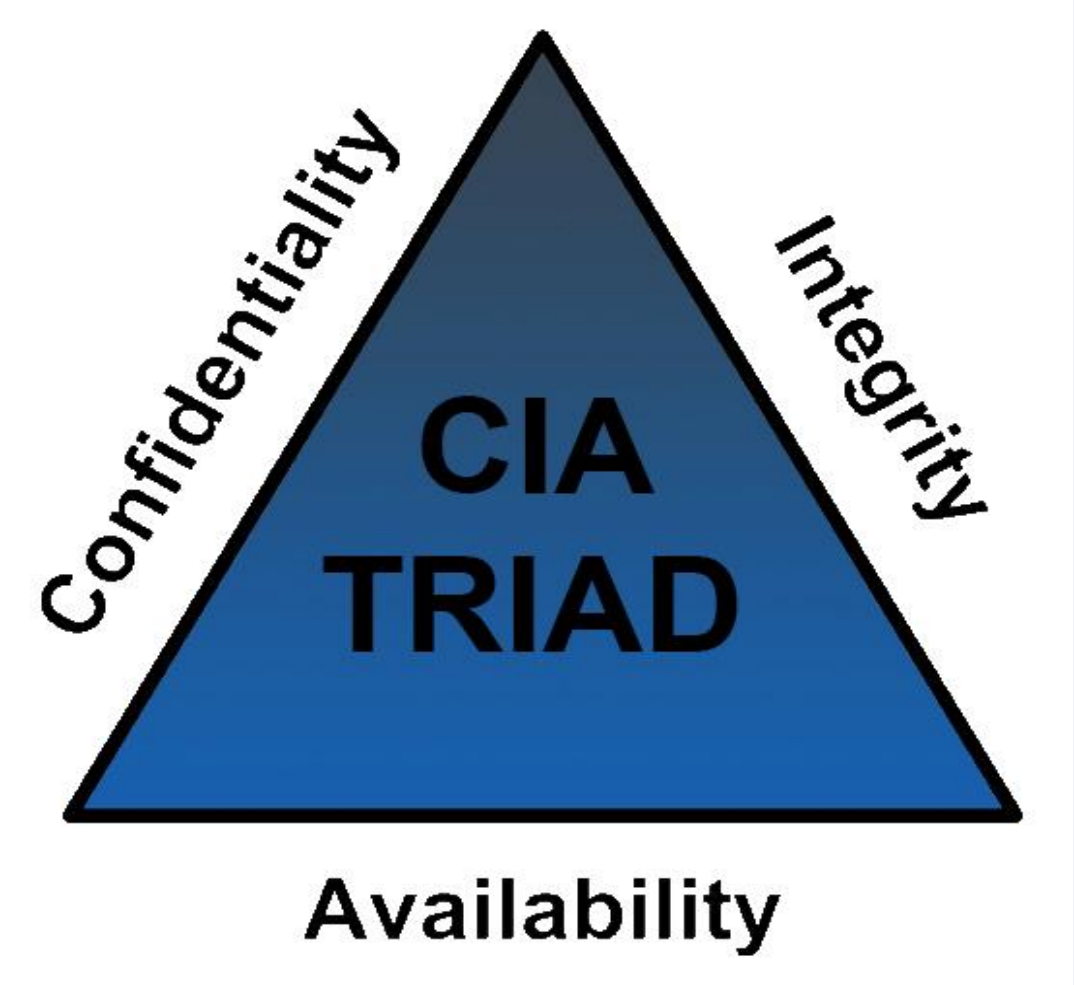
What is “AppSec”? In plain English

“Application Security is the art (or is that battle?) of making an application secure.”

-- Tanya Janca

The current state: Penetration Testing

The current state: CIA



OWASP
The Open Web Application Security Project

What is 'Pushing Left'?

If you imagine the SDLC written out on a piece of paper, the further left you go means the earlier you are in the SDLC process.

“Pushing Left” means security wants to be invited to the party earlier. And for AppSec, this means during the development phase.

Pushing Left, Like a Boss!

OWASP
The Open Web Application Security Project

An AppSec Program: The Main Course

An AppSec Program: The Main Course

- Vulnerability (VA) Scans and Assessments
- Threat Modeling
- Secure Code Reviews (Static Code Analysis)
- Penetration Tests (PenTests)
- This applies to both Custom Apps and COTS

An AppSec Program: The Gravy

An AppSec Program: The Gravy

- Educating Developers on Secure Coding Practices with workshops, talks, lessons
- Secure Coding Standards
- Responsible/Coordinated Disclosure
- Secure code library and other reference materials

An AppSec Program: Dessert!

OWASP
The Open Web Application Security Project

An AppSec Program: Dessert!

- Bug Bounty Programs
- Capture The Flag (CTF) contests
- Red Team Exercises

OWASP
The Open Web Application Security Project

The big question…

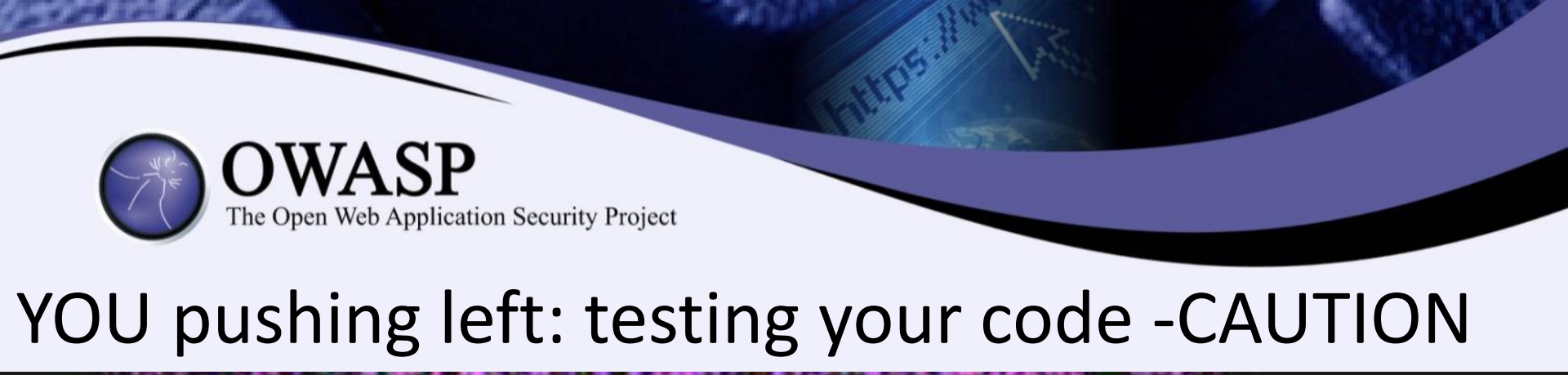
How can **YOU** push left?

OWASP
The Open Web Application Security Project

YOU pushing left: testing your code

YOU pushing left: testing your code

- Most people use a web proxy security scanner to test their web applications
- It sits between your browser and the internet
- It will automate tests for you, tell you what to fix, and, if it's a good one, HOW to fix the issues
- There are paid and free options available
- Don't use a scanner on an app you don't have permission to test, it's illegal

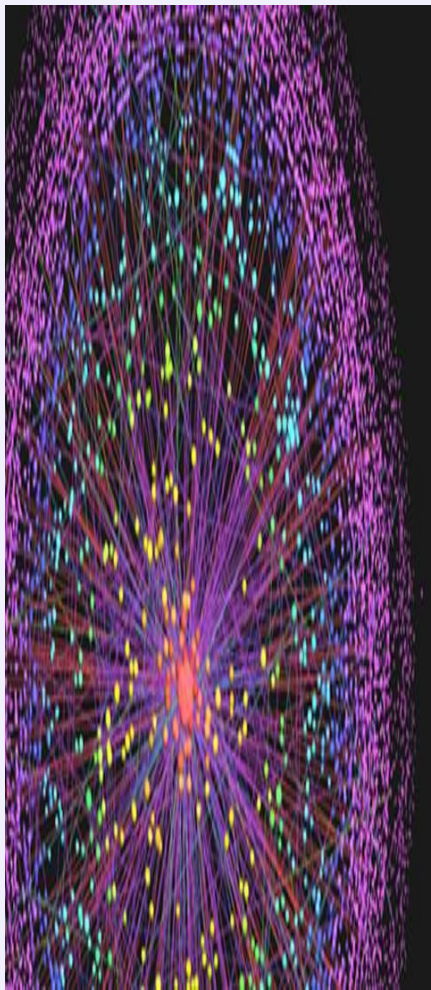


YOU pushing left: testing your code -CAUTION

OWASP
The Open Web Application Security Project

YOU pushing left: testing your code -CAUTION

- Ensure you have permission from your boss before you start, there may be policies against it (ask the security team too!)
- Be considerate, scanners can hog resources
- Be careful, scanners can be destructive
- Back up your data before hand
- This is an activity that requires some learning before you can start, to ensure you don't cause any damage or tick anyone off
-



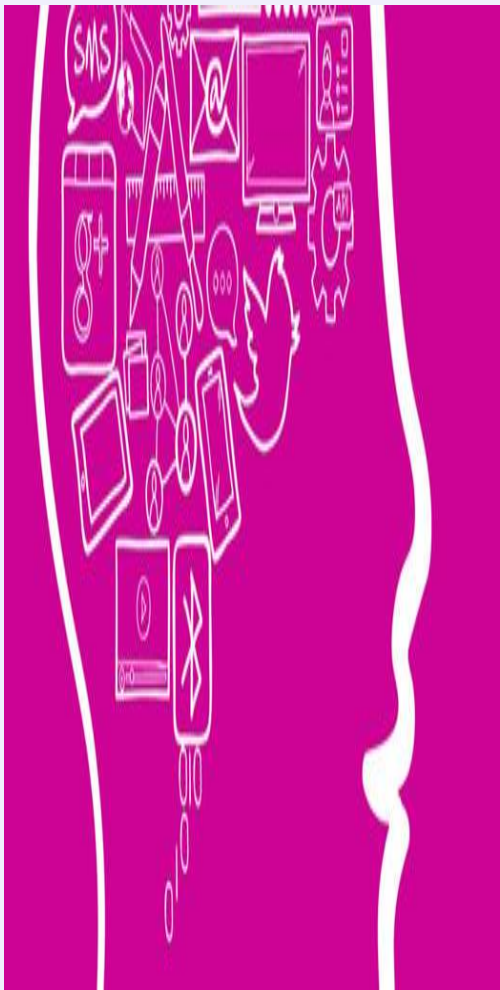
OWASP
The Open Web Application Security Project

YOU Pushing Left: Threat Modelling

OWASP
The Open Web Application Security Project

YOU Pushing Left: Threat Modelling

- Figuring out negative use cases, and ways to defend against them
- Basically a brainstorming session with programmers and security to figure out how someone may try to abuse your app
- Search you code for these threats
- Thinking like an adversary can not only uncover potential issues, it can be fun and educational.



OWASP
The Open Web Application Security Project

YOU Pushing Left: Reviewing your code

YOU Pushing Left: Reviewing your code

- Most people use a static code analyzer, but this can also be done manually
- Search for your threat models
- Even the most expensive tool produces many false positives, the 'work' in this exercise is figuring out what is a real issue and what is not
- OWASP Dependancy check
- You can find more than just security bugs

OWASP
The Open Web Application Security Project

YOU Pushing Left: Writing better code

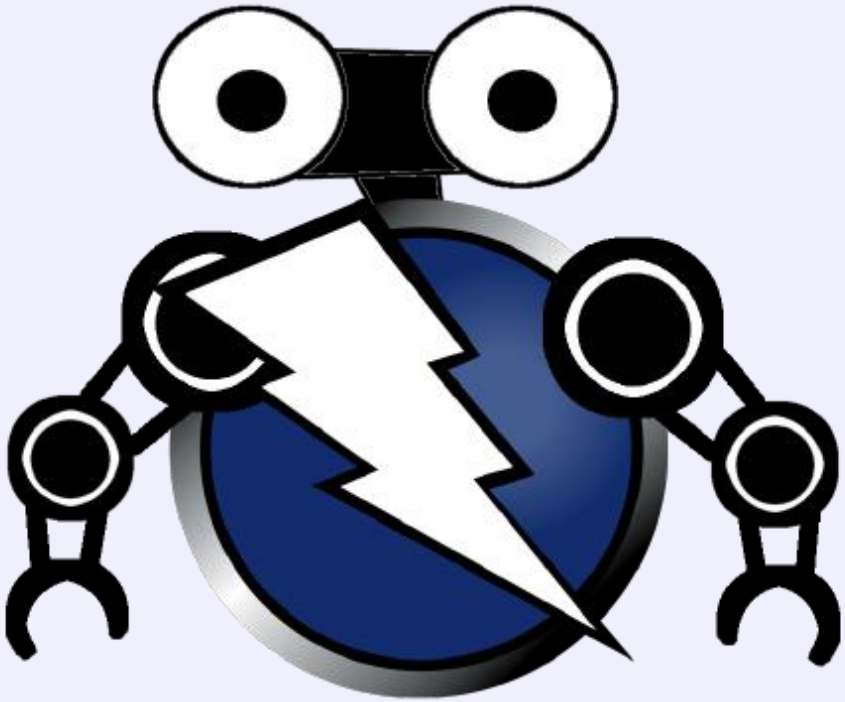
OWASP
The Open Web Application Security Project

YOU Pushing Left: Writing better code

- Train yourself on secure coding practices
- There are tons of quality online resources, free and paid, as well as courses and conferences
- Check online for the best and most secure way to do things, before you start coding
- Become the security expert on your dev team, and help the rest of your team learn

OWASP
The Open Web Application Security Project

OWASP: Your new BFF



OWASP
The Open Web Application Security Project

Open Web Application Security Project

ANY QUESTIONS?

Tanya Janca

Tanya.Janca@owasp.org

OWASP Ottawa Chapter Leader

OWASP DevSlop Project Leader

@SheHacksPurple