Gov-X Innovation Challenge 2021

Quis Custodiet Ipsos Custodes?

Carl Kritzinger

Developer, KnowBe4

Carl Kritzinger

Developer, KnowBe4

Background:

I build things
often with code
sometimes for money

1.
You’re not paranoid

They are out to get you

1 in 4

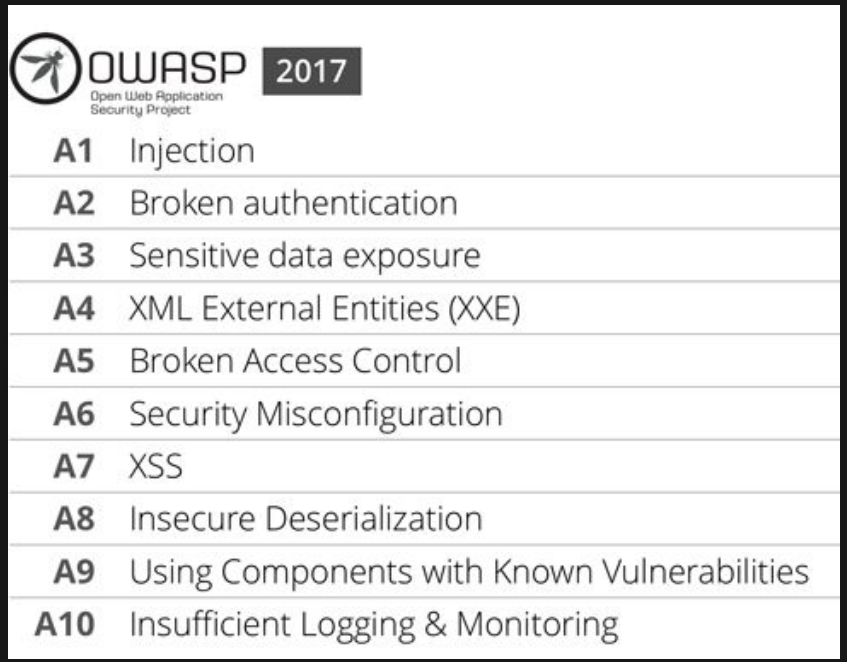
Companies had a breached web application in 2019

$4 Million

Average cost of a breach in 2020

2.
Here’s how

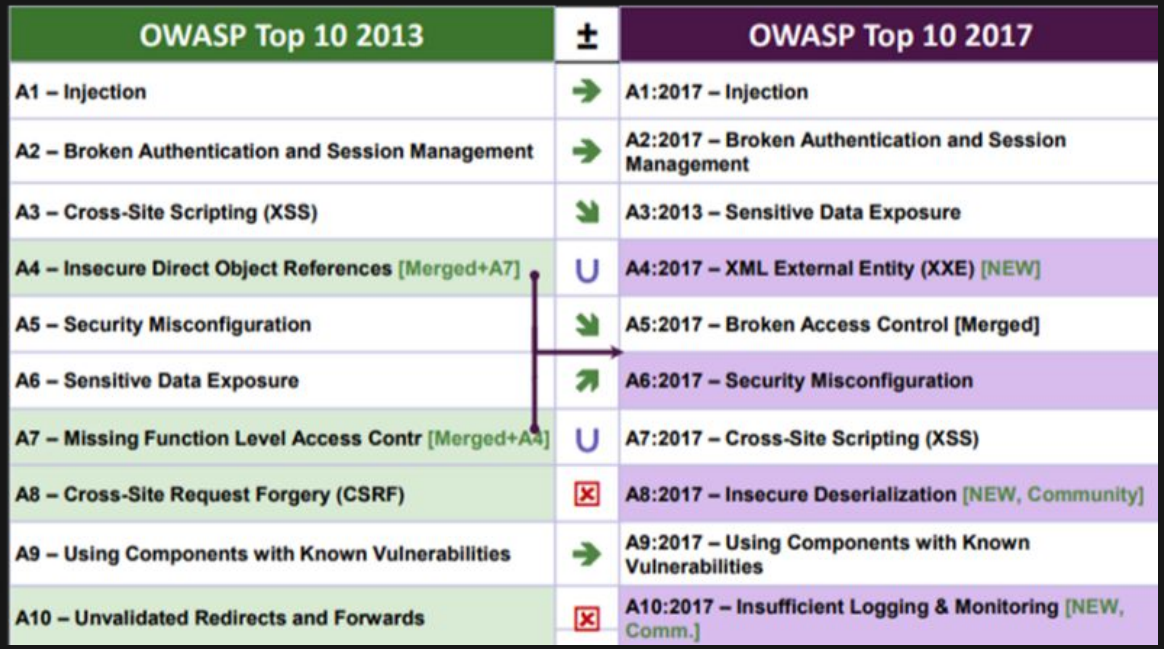
They’re going to get you



The OWASP Top 10 web app vulnerabilities

BUT WAIT

This talk will NOT teach you to be a secure developer



OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Injection	→	A1:2017 – Injection
A2 – Broken Authentication and Session Management	→	A2:2017 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	↘	A3:2013 – Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017 – XML External Entity (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017 – Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017 – Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017 – Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017 – Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017 – Insufficient Logging & Monitoring [NEW, Comm.]

Things change

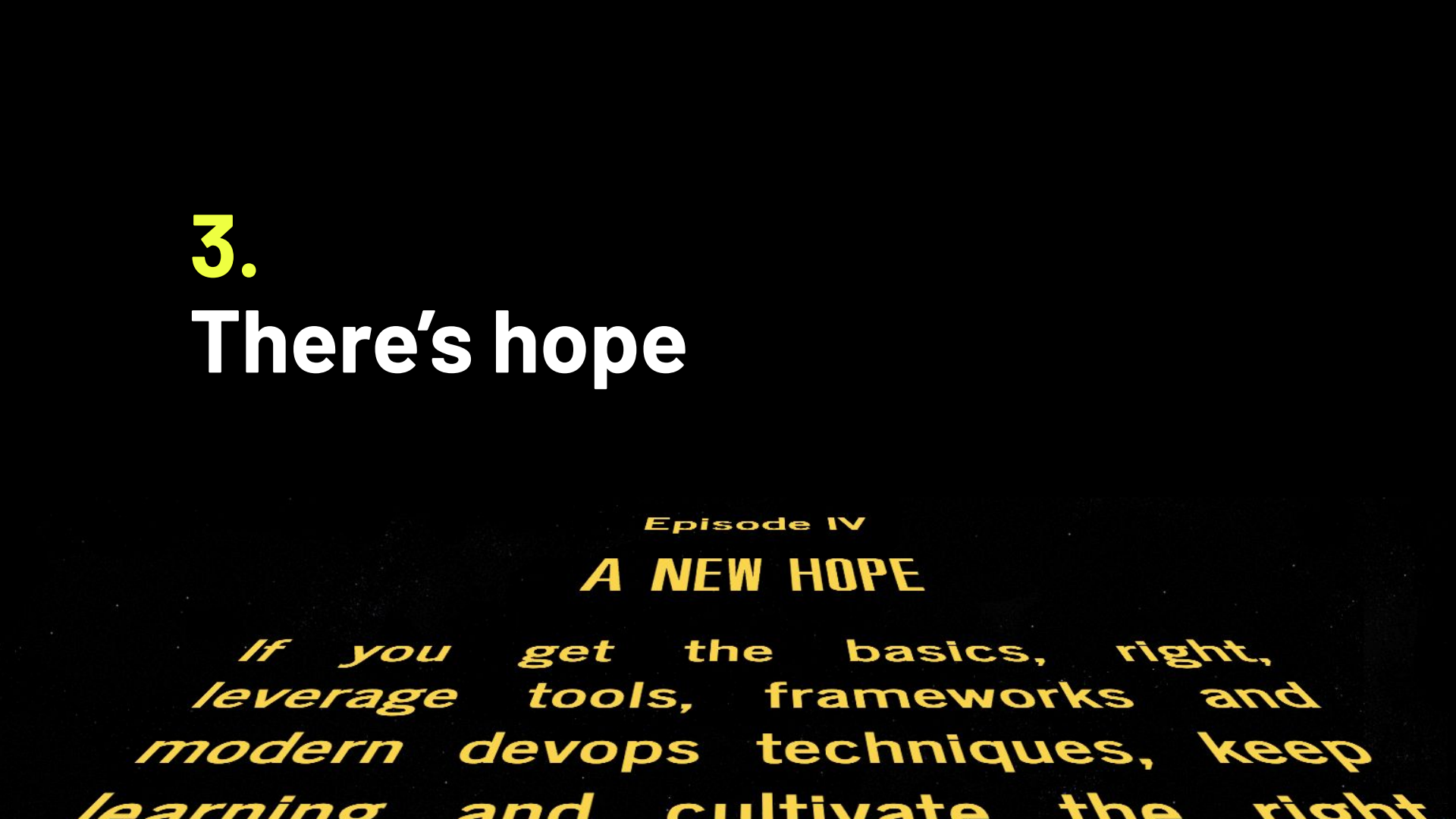
Often and a lot

A6	Security Misconfiguration
A7	XSS
A8	Insecure Deserialization
A9	Using Components with Known Vulnerabilities
A10	Insufficient Logging & Monitoring

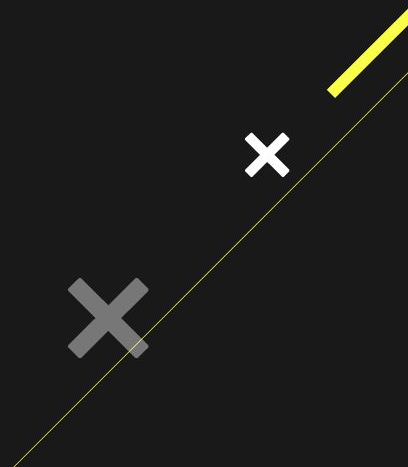
« ‹ 1 2 3 4 › »

Showing 1..10 of ∞

3.
There’s hope



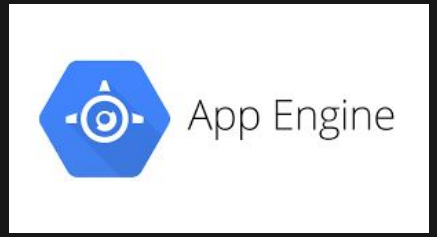
GET THE BASICS RIGHT



OWASP Top 10
Proactive Controls

1. Define Security Requirements
2. Leverage Security Frameworks and Libraries
3. Secure Database Access
4. Encode and Escape Data
5. Validate All Inputs
6. Implement Digital Identity
7. Enforce Access Controls
8. Protect Data Everywhere
9. Implement Security Logging and Monitoring
10. Handle All Errors and Exceptions

BE
LAZY

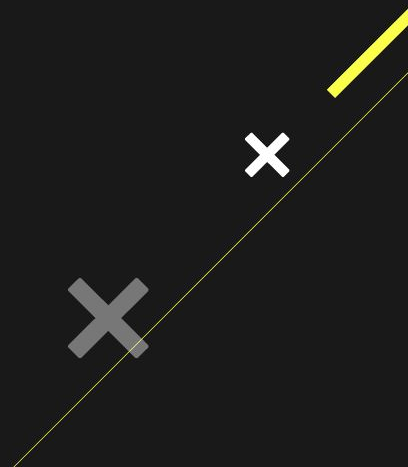


Don’t run your own infrastructure

Don’t write your own code*

*particularly not crypto/security code

Make it hard to FSCK up



“We become what we behold.
We shape our tools and thereafter
our tools shape us.”

Marshall Mcluhan

Tools

- Linters
- CI and Unit tests
- Static Analysis
- Dynamic Analysis

Processes

- Security Requirements
- Code Reviews
- Audits and Pen tests

Habits

- Think like a hacker
- Write clean code
- Stay up to date ($social_media_icons)

KTHXBYE

questions/comments?

mailto:carlk@knowbe4.com