Vulnerability Remediation

CHALLENGES AND PROPOSED APPROACH

NABIL HANNAN
MANAGING PRINCIPAL, CIGITAL INC.
NHANNAN@CIGITAL.COM

@nabilhannan

 |

We Can't Test Ourselves Secure

- Test coverage is low
  - Even with IAST [knight in shining armor]
- No one testing technique finds even all critical vulnerability (types)

cigital

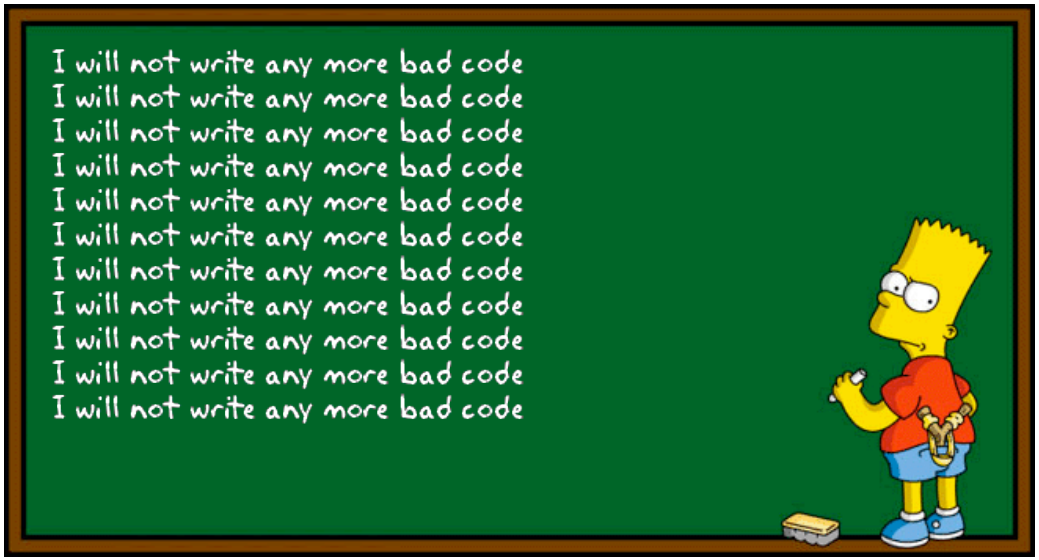
[Anyways,] We Know It Doesn't Work

- 10+ years, our re-exploit rate remains incredibly high
  - Where vulnerabilities are closed, re-exploits through [simple] evasion is common

cigital

Easier Done Than Said?

- Pick a few common problems
- Solve them
  - Password Storage
  - CSRF protection
  - Encoding



cigital

The Right Way To Do It

1. Seek existing secure code from within the organization
2. Extract that code to shared libraries
3. Bake libraries into existing Web/ORM/ etc. frameworks
4. Make sure frameworks apply protection…
   - As part of functional operation
   - Automatically, w/o developers calling it
   - Possess secure-by-default

cigital

ESAPI #YouAreDoingItWrong

- Pick an un-maintained library
- Adopt an “API” that developers have to:
  - Remember to call, everywhere necessary
  - Choose the right function to call
  - Configure each call correctly

cigital

Measuring / Assuring Progress

- Use (open source) SAST to measure use
- Unit test for consistent, complete & correct use
- Lend teams bandwidth/expertise to integrate
- Reward developers (ease assessment) for use
- Build and tell success story

cigital

Thank You

NABIL HANNAN
MANAGING PRINCIPAL, CIGITAL INC.
NHANNAN@CIGITAL.COM


@nabilhannan

