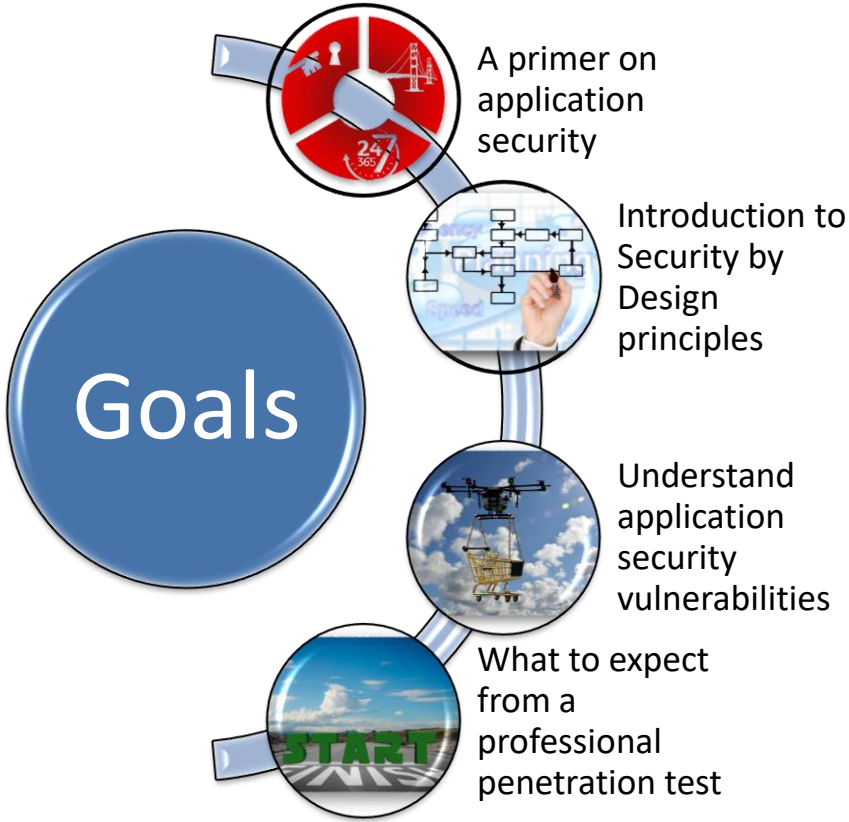
Foundational Application Security Training

Secure Ideas, LLC

What are the Goals of FAST?



People Trust the Web With Everything

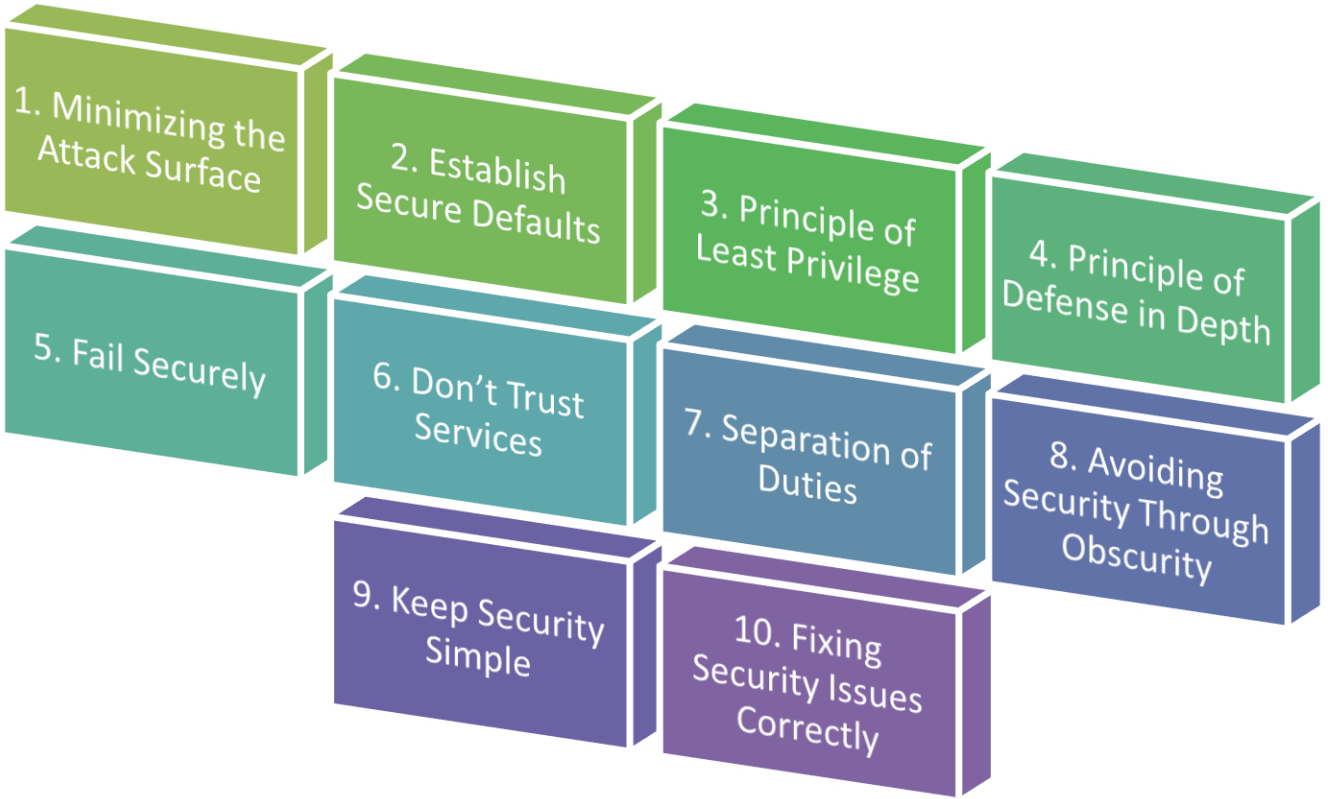
The CIA Triad

Confidentiality

Integrity

Availability

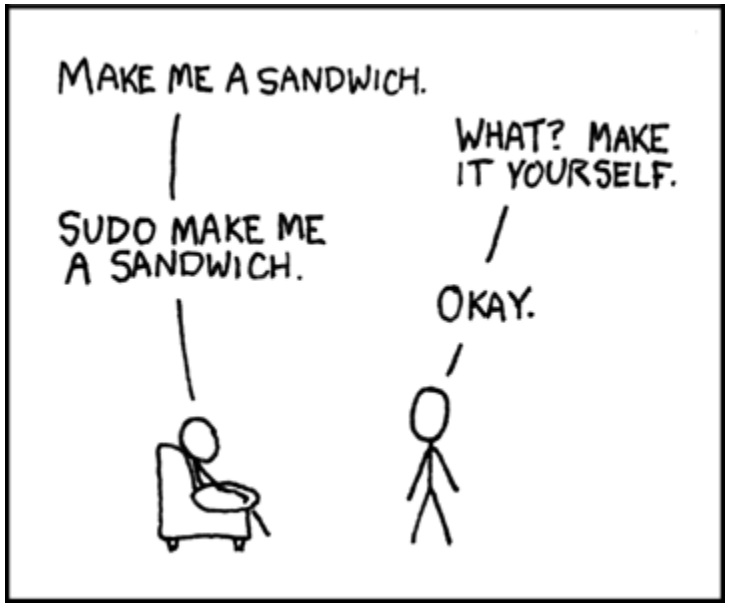
OWASP Security by Design Principles



Source: https://www.owasp.org/index.php/Security_by_Design_Principles

Principle of Least Privilege

- Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.
  - Jerome Saltzer (Computer Scientist)



Source: https://xkcd.com

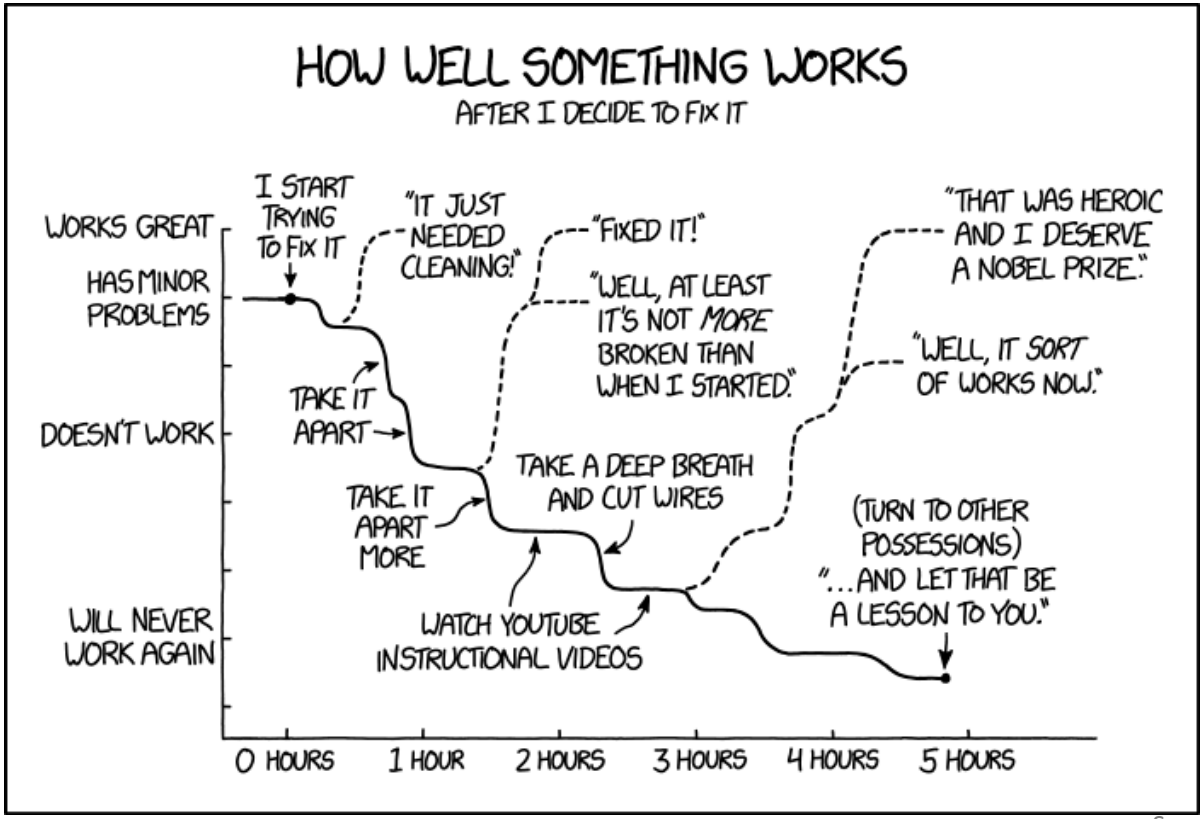
Principle of Defense in Depth

- Also known as the Castle Approach
- The defensive concept of using layers of security controls

Why is this important?

→ Because *no* control is ever considered 100% effective!
→ Security controls are regularly circumvented

Fix Security Issues Correctly



Source: https://xkcd.com

OWASP Top 10 Proactive Controls (2018)

Written by developers for developers, the controls are:

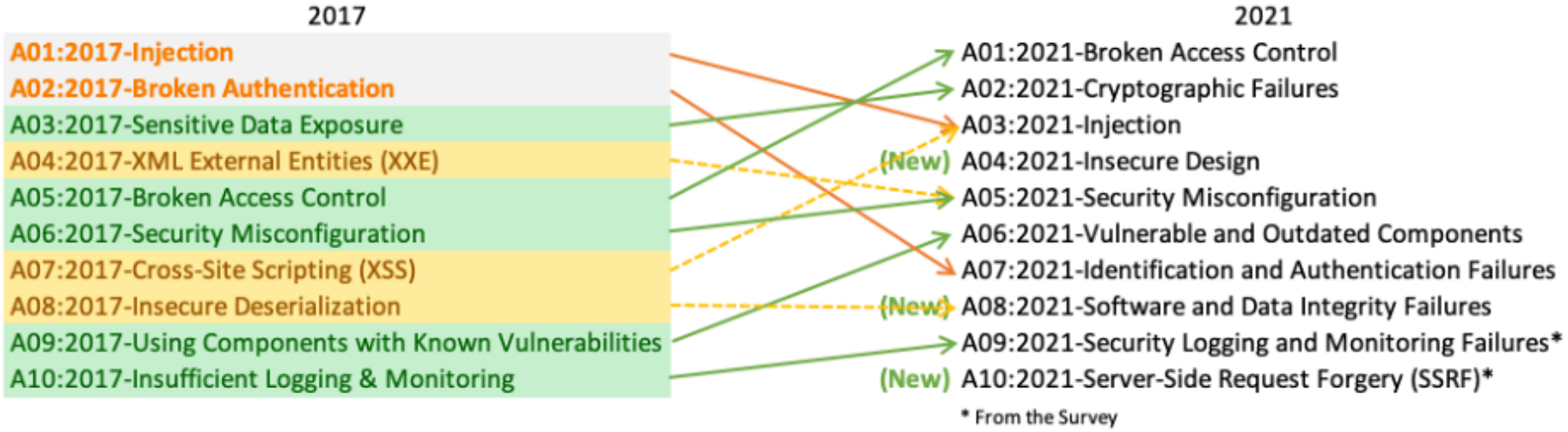
1. Define Security Requirements
2. Leverage Security Frameworks and Libraries
3. Secure Database Access
4. Encode and Escape Data
5. Validate All Inputs
6. Implement Digital Identity
7. Enforce Access Controls
8. Protect Data Everywhere
9. Implement Security Logging and Monitoring
10. Handle All Errors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

OWASP Top 10 - 2021
Critical Application Security Risks

A1 – Broken Access Control
A2 – Cryptographic Failures
A3 – Injection
A4 – Insecure Design
A5 - Security Misconfiguration
A6 – Vulnerable and Outdated Components
A7 – Identification and Authentication Failures
A8 – Software and Data Integrity Failures
A9 – Security Logging and Monitoring Failures*
A10 – Server-Side Request Forgery (SSRF)*

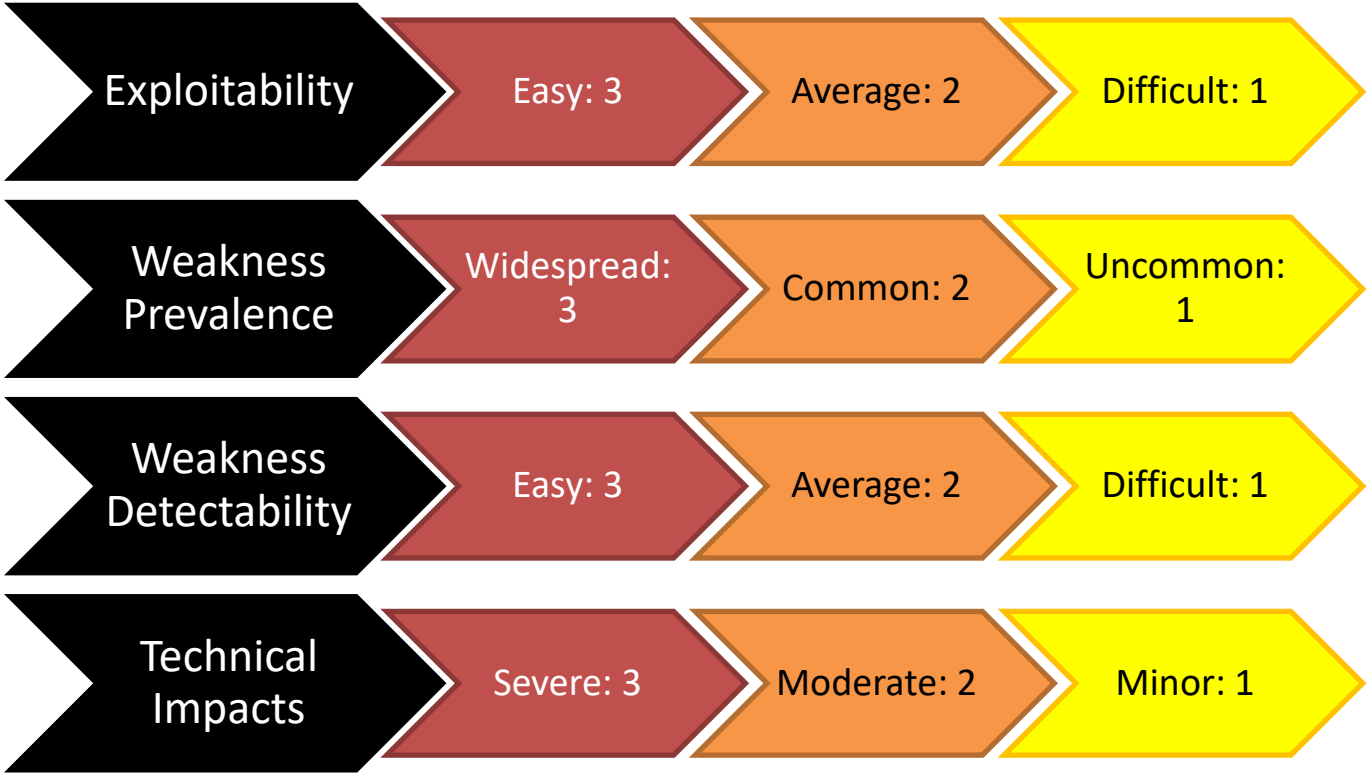
* From a Survey

Changes from 2017 -> 2021



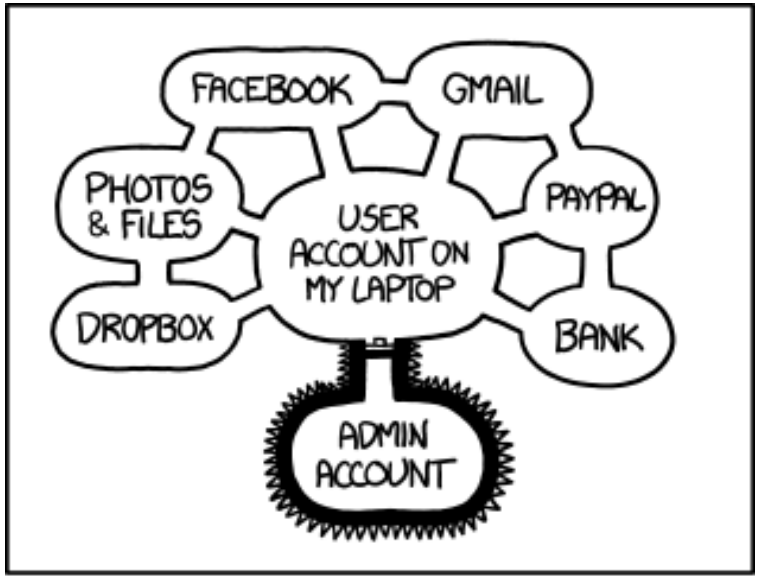
Source: https://owasp.org/www-project-top-ten/

OWASP Top 10 Risk-Rating System



Note: ***Threat Agents*** and ***Business Impacts*** are also listed but not rated.

What is access control?



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Source: https://xkcd.com

What is an Injection Flaw?

Consider a Drone delivery system…

1. Get package
2. Read address label
3. Deliver package
4. Return home
5. Go to step 1

What if?

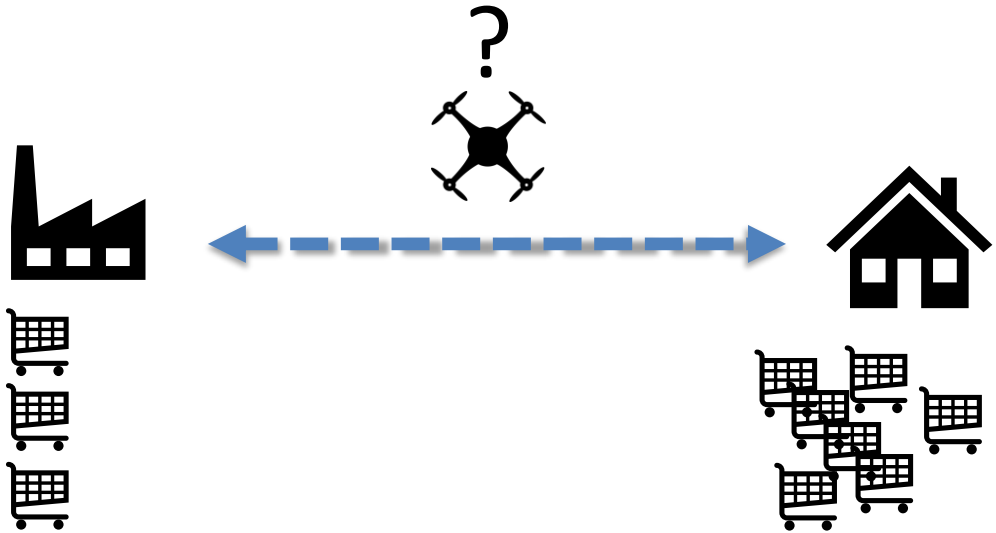
1. Get package
2. Read address label

3412 Kori Rd.

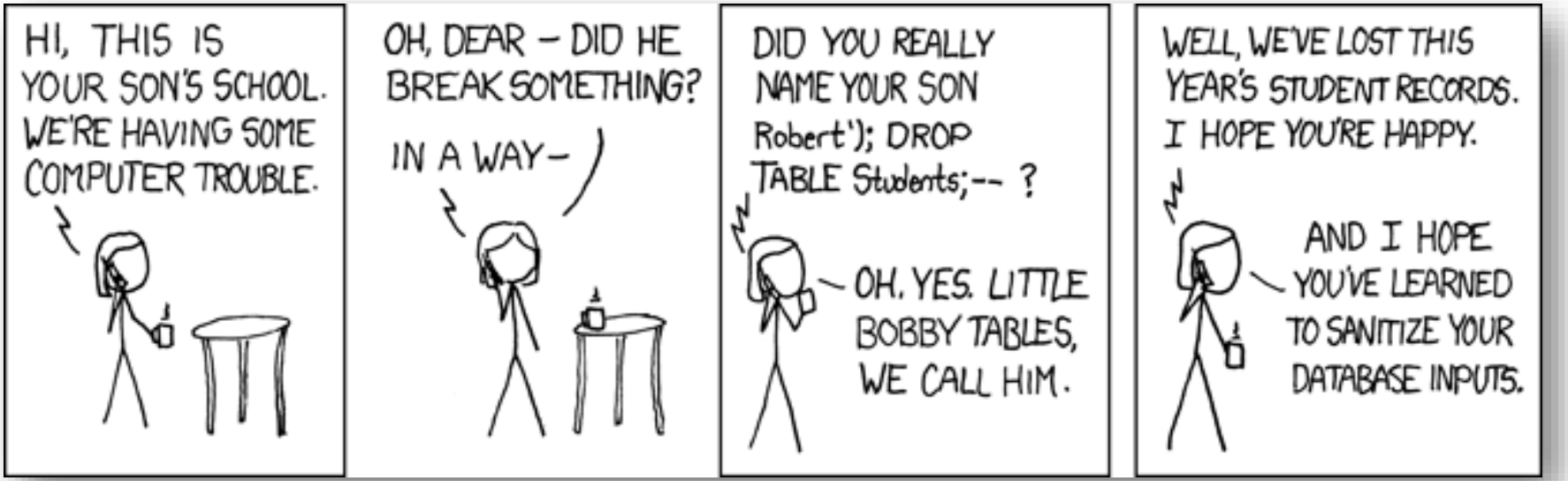
Jacksonville, FL

```
3.Deliver package
4.Return home
5.Get package
6.Go to step 3
```

3. Deliver package
4. Return home
5. Go to step 1

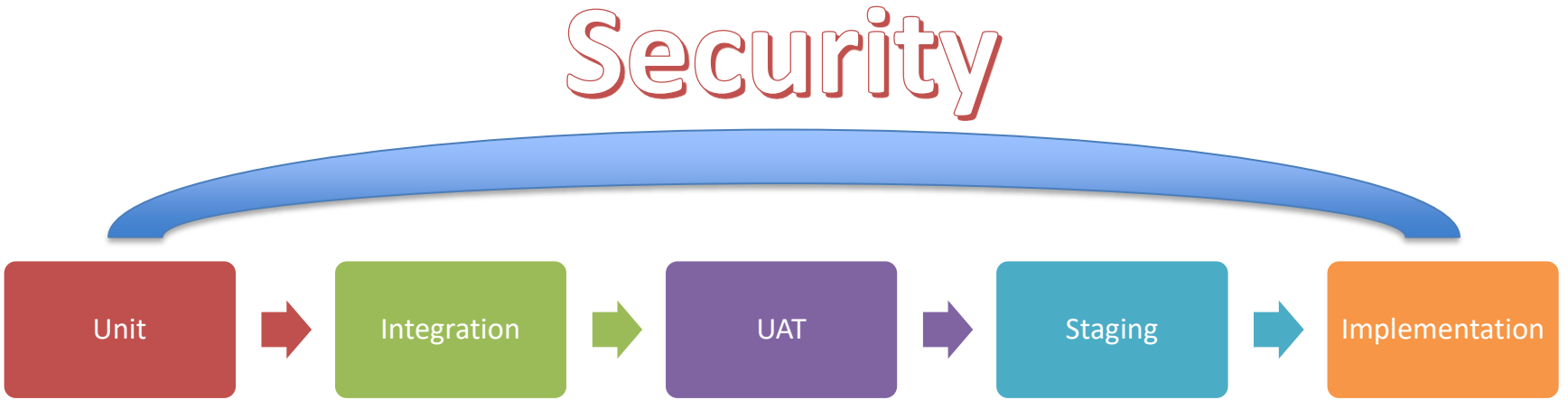


SQL Injection



Source: https://xkcd.com

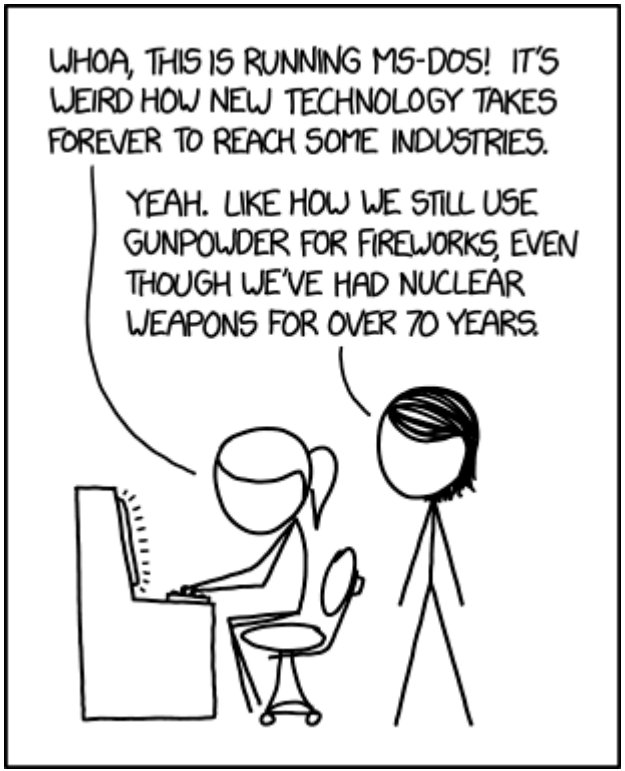
Testing



What is monitoring?

Source: https://xkcd.com

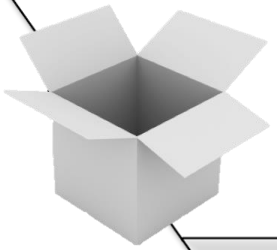
Scoping: Technology



- Technology stack
- Define application boundaries
- Is any attached infrastructure in scope?
- Any services? (e.g. OAuth, Message bus)

Source: https://xkcd.com

Test Type

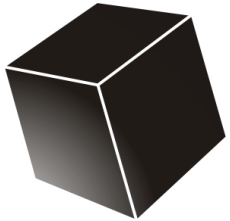


White Box

- Source code
- Detailed architecture
- Developers

Gray Box

- Accounts
- High-level architecture



Black Box

- Location (URL, hosts)

Any Questions?