

Secure Software Development | Ivan Notes 2022

Databases

Components of DBMS

- hardware
- software
- tables
 - rows = tuples/records
 - column = attribute
 - field = intersection of row + column
- primary & foreign keys
 - primary = unique identifier
 - foreign = relationship to PK
- Language (SQL)
- Users
- Data

Maintaining data integrity

- concurrency
- use locks
- ACID
 - atomicity
 - consistency
 - isolation
 - durability

System life cycle (SLC) | SDLC focuses in 1-6

1. Plan & approval
2. reqs analysis
3. design
4. development
 - waterfall — cant go back
 - agile
 - sprints
 - scrum master
 - devops
 - combine dev, QA, & ops
 - secdevops
5. testing
 - canary deployments
 - product certification
6. deployment — accreditation
7. operation
8. disposal

Maturity Models

CMM, CMMC

APIs

- REST
- SOAP

Secure programming

- input validation
- session management
- polyinstantiation

Code obfuscation

lexical, data, control flow

Acquiring software

- assess vendors
- contracts / SLAs

Weaknesses & Vulns

- buffer overflows
 - protect with ASLR
- SQL injection
 - prevent with input validation
- XSS / CSRF
 - stored = persistent
 - reflected = more common
 - xss targets browser, CSRF targets web app
- covert channels
 - storage = more common
 - time
- backdoors
- memory / object reuse
- TOCTOU (race conditions)
- citizen developers