

Penetration Testing

Testing the functionalities

- ✓ Unit test, Integration test, Performance test and so on ...

Testing the security

- ✓ Penetration tests

- ➔ Try to make the software fail by pushing the limits of a “normal” usage i.e test what the program is not supposed to do

Vulnerability Detection

- **Static analysis (SAST)**
Analyze source or binary without running it
- **Fuzzing**
Automatically input generation to crash/trigger bugs
- **AI** (newest trend)
Uses LLM to understand code behavior and identify vulnerabilities
Aardvark (OpenAI) and Big Sleep (Google)