SAST for a More Secure Future -- Today

Nathan Larson

Alex Bauert

Agenda

- What is SAST?
- Why SAST?
- SAST as a silver bullet
- If the automated tools are so good, why do we need an AppSec team?
- Incorporating SAST into the build process
- The Results

What is SAST?

- Static Application Security Testing
- Analyze source code without execution
- Look for patterns
  - Vulnerabilities
  - Dangerous data handling
  - No logic flaws
- Types
  - Manual
  - Automated
- SAST is not SCA or IAST

Why SAST?

- DAST, pen testing can catch many defects
- SAST can catch many too
- SAST tools typically look for:
  - User controlled (tainted) data
  - Data flow defects
  - Source code syntax problems
  - Specific vulnerabilities

Why tool-assisted SAST?

SAST tools

- Typically contain thousands of rules
- Scan code tirelessly
- Scan code quickly
- Scan consistently

People

- Can remember classes of vulnerabilities
- Tire/bore easily
- Parse code slowly
- Test inconsistently

Can you parse MBs of code in an hour without breaks, then do it again a month later with the same results?

SAST as a silver bullet

- Spoiler alert: it isn't
- Automated tools return false positives
- The real work is triaging the results
- Not every finding is exploitable

- Better to see as *part* of a security program
  - Complements pentesting, DAST, IAST
- SaaS or on-Prem
  - why is SaaS so much faster?

Why need AppSec professionals?

- The tools are that good, right?
- Remember the false positives?
- Why not just let devs triage and fix?
- Tuning the engine

- Need to verify and triage findings
  - Training
  - Practice
  - Context: every company/app different

Scanning as part of the build

- Script into the build process
- No manual scans needed
- Automate scans to “shift left”
- Allow dev teams to fix earlier

Results

- The PDF file
  - Triage with the dev team
  - Context
  - Remediation
- Automation
  - Thresholds for stopping the build
  - What are the showstoppers
- Time to fix
  - Remediation, compensating control or risk acceptance
- Retesting

Reporting

- What are you trying to communicate
  - Severity and volume
  - Categories
  - Open and time to close
  - Remediation, compensating control or risk acceptance
- Demonstrate effectiveness
  - Baselining and plateaus
- Hybrid Reporting

Thank you

What's next?

- Research something you want to share?
- Have lots of knowledge about a topic?
- Just love appsec so much, you can't help it?

OWASP chapters always need speakers!
See the Meetup group for info