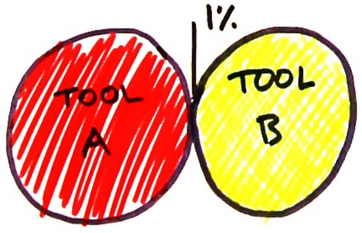
COMMONALITY AND TRENDS IN SAST RESULTS

Chris Near

IF YOU'RE USING ONLY 1 OR 2 TOOLS, YOU'RE REALLY MISSING A LOT.



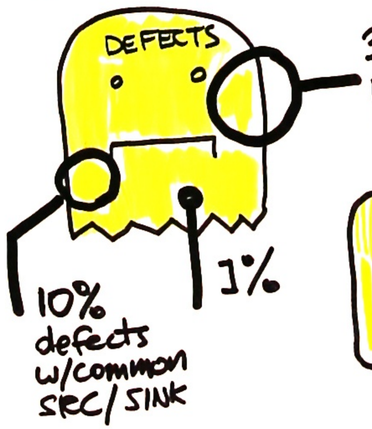
LESS THAN 1% OVERLAP IN DEFECTS FOUND BY DIFFERENT AST TOOLS

UNDERSTANDING ONE TOOL DOES NOT MEAN YOU'LL UNDERSTAND ANOTHER ONE

DEFECT COMMONALITY

- DEFECT NORMALIZATION
- DE-DUPLICATION
- COMMON SINK-SOURCE LOCATION
- PARENT-CHILD RELATIONSHIPS
- CAUSE-EFFECT RELATIONSHIPS

SAST COMMONALITY



Open source tools are often better at minimizing false positives than commercial tools

THE MORE BROAD THE RULE, THE MORE LIKELY YOU'LL HAVE FALSE POSITIVES

SAST FOCUSES ON HARD-TO-EXPLOIT DEFECTS

FALSE POSITIVE TRENDS

- JAVA IS HIGHLY ACCURATE
- C++ IS NOT

EASE OF EXPLOIT TRENDS

- NEEDED MORE THAN ONE DEFECT FOR AN ATTACK
- FEW DEFECTS ARE EASY TO EXPLOIT

SEVERITY

- BELOW 90, MEDIUM CONSEQUENCE
- "C" LANGUAGES HAD HIGHER LEVELS OF SEVERITY

→ USE LOTS OF TOOLS! ←