Finding Bugs

- Symbolic Reasoning [15]
- Compositional Approach [1, 31]
- Static String Analysis to generate potential HTML output [23]
- Implementation based Testing [9, 10, 12, 17, 29]

Better Branch Coverage

- Hybrid Concolic Testing [21], evolutionary testing [18], white-box fuzzing [16]

Combining Concrete and Symbolic Execution

- Improving Scalability [1, 13, 14, 16, 22]
- Improving Execution Coverage & Fault Detection [5, 11, 16, 18, 21, 28]

Delta Debugging [6, 34, 24]

- Exploiting Program Input Structure [22]

Identifying minimal set of variables that induce failure

This Paper

Uses an oracle, minimizes constraints on inputs, first in proactive fault detection of PHP Web applications