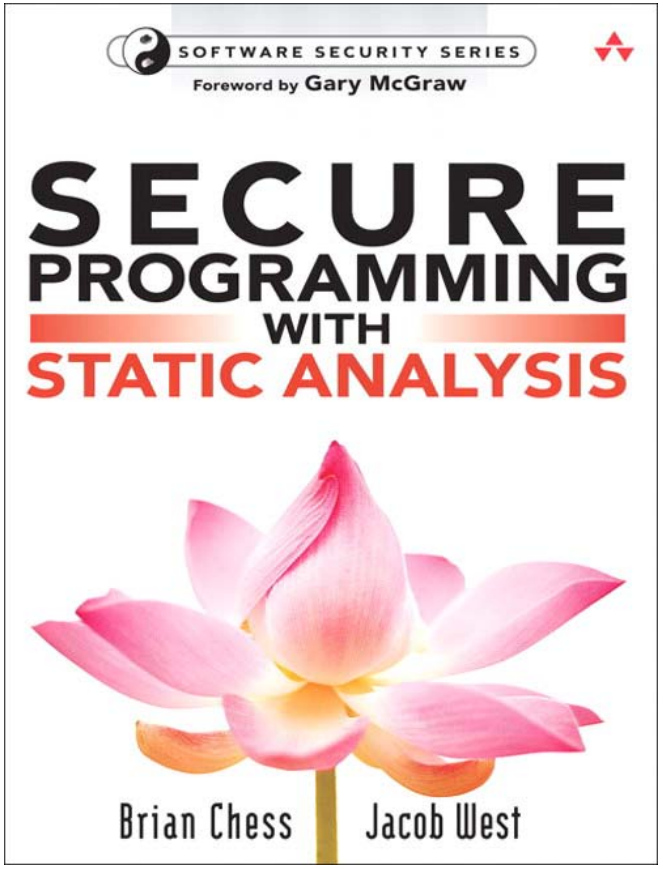
Real-Time Hybrid Analysis

Brian Chess
chess@hp.com
March 8, 2011

TRUST YOUR SOFTWARE™

Brian Chess

- Founder/Chief Scientist Fortify Software
- Ph.D. from University of California Santa Cruz
- Loves:
  “Success is foreseeing failure”
- Hates:
  “The only way to stop the bad guys is to hunt them down and sue them until they stop.”



Dynamic Testing & Static Analysis: Pros and Cons

Dynamic Security Testing

- Advantages
  - Concrete results
  - Tests real environment
- Disadvantages
  - Little insight into root cause
  - Limited by test coverage

Static Security Testing

- Advantages
  - Comprehensive results
  - Source-level details
- Disadvantages
  - No exploit provided
  - Prioritization difficult

Example: correlating SQL Injection findings

Dynamic Result

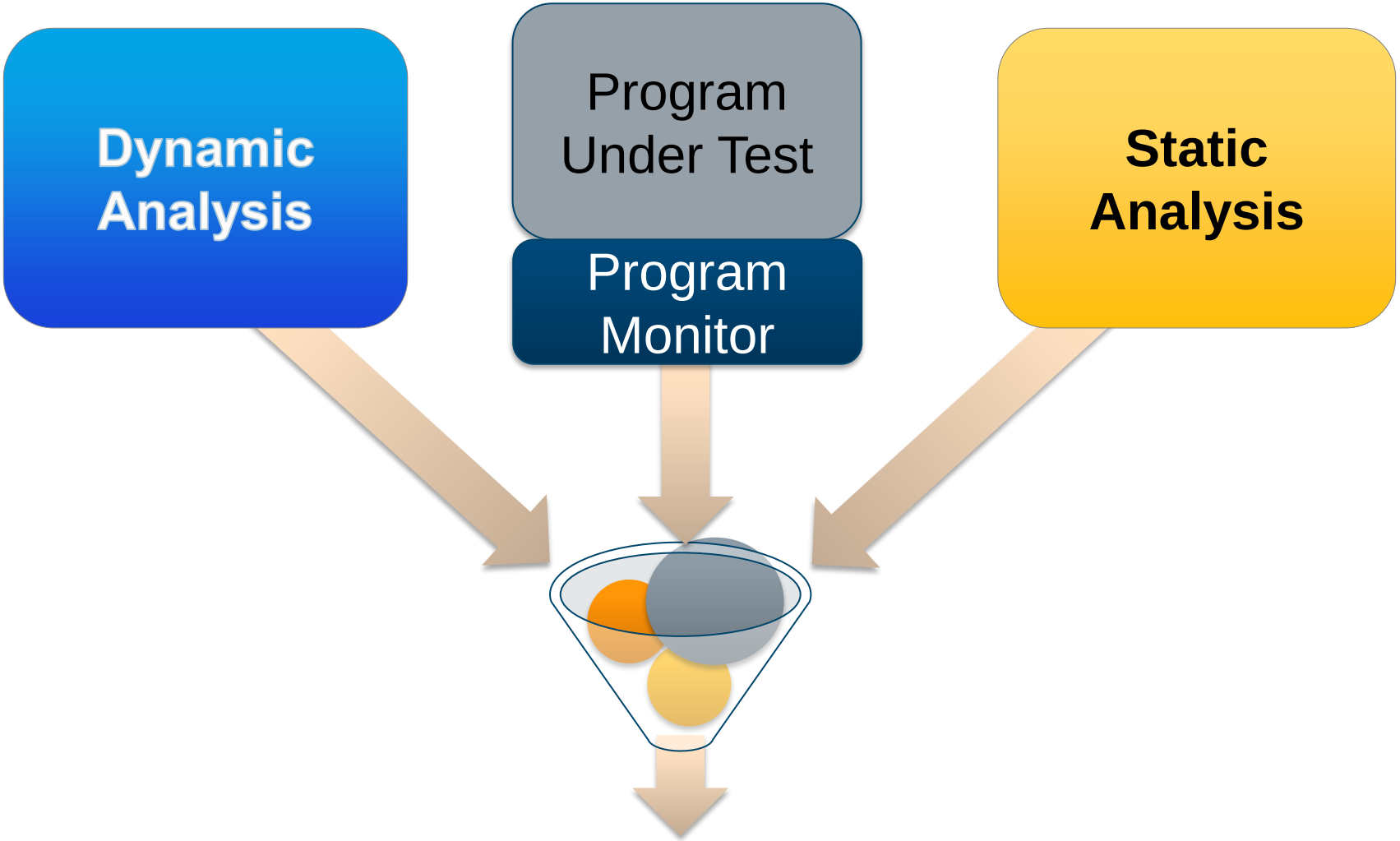
Attack:
http://www.
sales.company.com?
x=Robert'); DROP
TABLE Students;--

Static Result

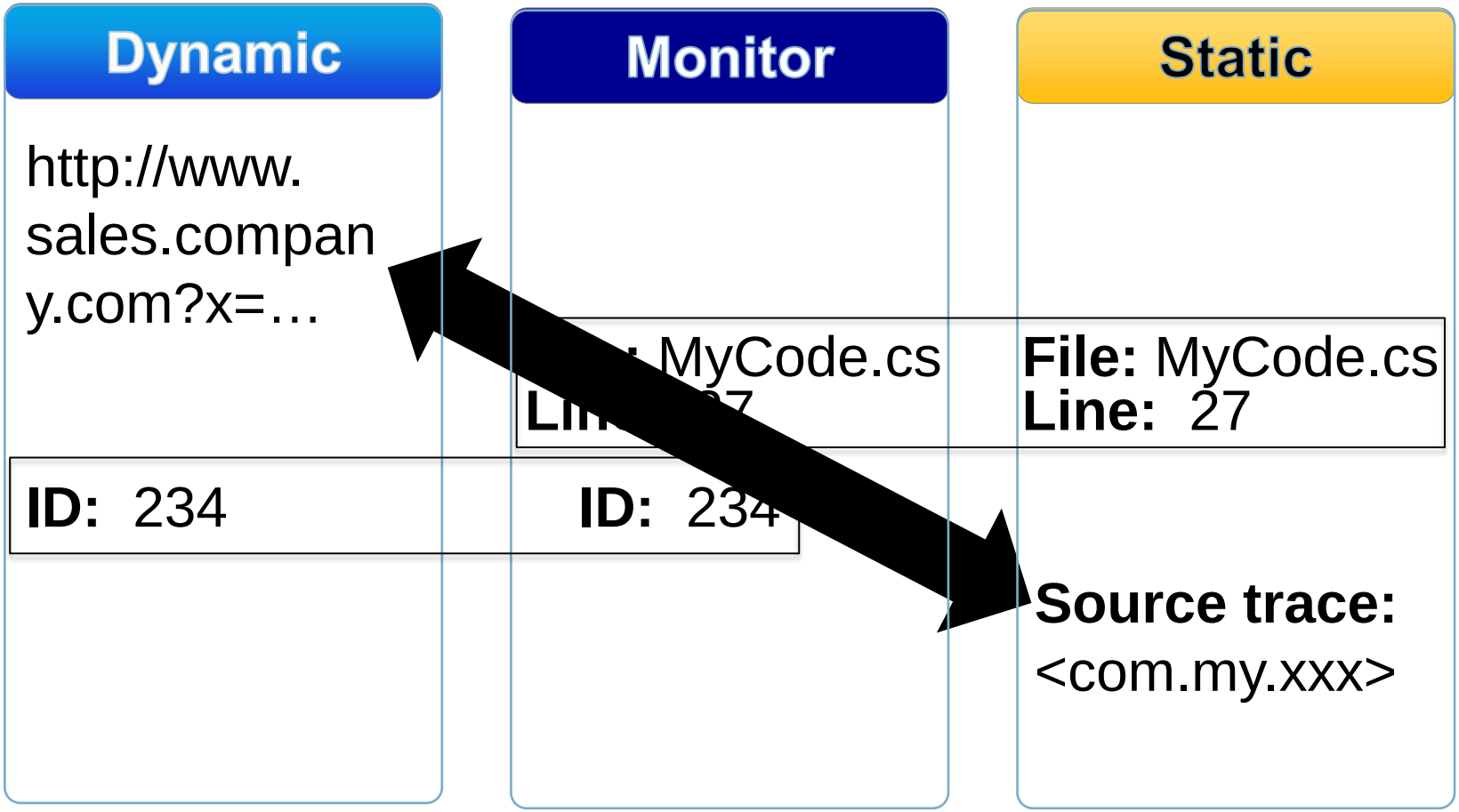
File: MyCode.cs
Line: 27

Source trace:
<com.my.xxx>
<com.my.yyy>
<com.my.zzz>

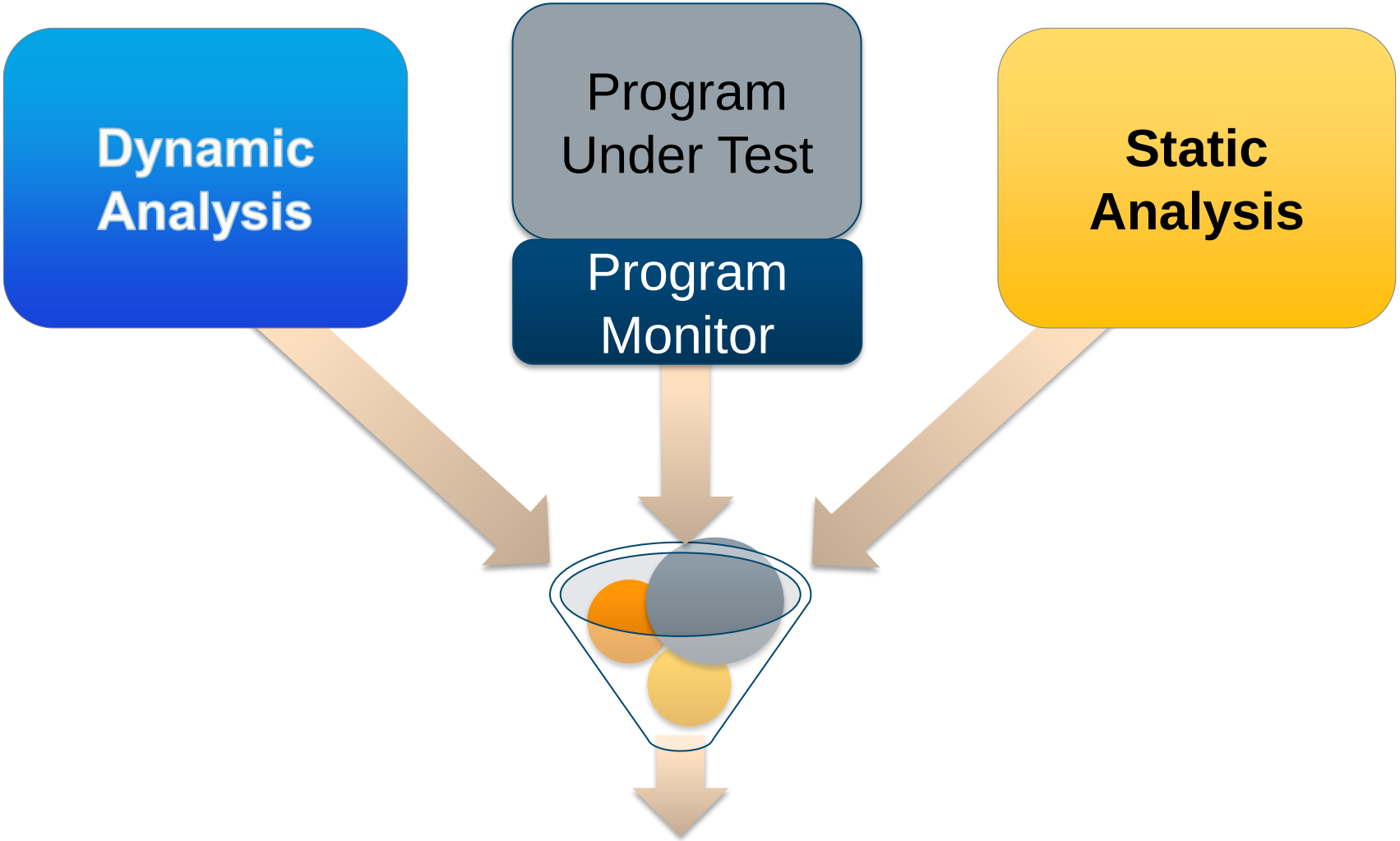
Architecture



Example: lining up SQL Injection findings



Architecture



Real-Time Hybrid Analysis

Brian Chess
chess@hp.com
March 8, 2011

TRUST YOUR SOFTWARE™