

How are vulnerabilities discovered?



Source code auditing



Fuzzing





Program analysis (synthetic, static and dynamic)

Vulnerability Discovery and Disclosure

Vulnerability Discovery and Disclosure

- ◎ How are vulnerabilities discovered?
 - ➡ Source code auditing
 - ➡ Fuzzing
 - ➡ Variant analysis
 - ➡ Program analysis (synthetic, static and dynamic)

Vulnerability Discovery and Disclosure Contd.