1. What is static code analysis?

It is method of debugging

1. When SCA is performed?

It is performed early development before actual testing begins.

1. Why SCA?
2. Can review source code methodically
3. Can follow coding standards and RCA learning
4. Help to understand complex code
5. Can find most common defects at desktop
6. 100% coverage
7. Manual code review effectiveness goes up
8. Reverse engineering code becomes easy
9. You can focus on functionality in code review
10. Advantages of SCA:
11. Helps identifying software quality issues during development and complex issues than compilers can.
12. Detects the code that needs to be simplified
13. Detects programming error
14. Improves communication between development team to produce high quality code
15. Kind of Defects:
16. Security issues
17. Application crashes
18. Memory leaks
19. Other leaks

Example:

1. Buffer overflows: security exploit or program crashes
2. Null pointer dereferences : program crashes
3. Memory leaks: processor runs out of memory and locks up
4. Unlimited data usage: data injection
5. Platform/OS specifics : privilege escalations
6. Concurrency: Deadlock
7. Suspicious coding practices: Variable assignments, function calls