Abstract

Static code analysis is a software verification activity in which source code is scrutinized for quality and security. In a Software Development Lifecycle, timely detection of flaws is beneficial and static analysis tools help us to detect flaws at a very early stage. Both commercial and open source static analysis tools are available today. Due to diverse user requirements and capabilities of the tools, a comparison between tools is required. Three open source static analysis tools for security are evaluated in this paper. These are Cppcheck, RATS and Flawfinder. They have been studied and compared to each other on the basis of detection ratio. For the purpose of obtaining the detection ratio, the vulnerabilities were categorized and intentionally introduced into the demo codes.

References

Comparing Detection Ratio of Three Static Analysis Tools


19. RATS Information Website. URL: https://code.google.com/p/rough-auditing-tool-for-security/

20. Flawfinder Website. URL: http://www.dwheeler.com/flawfinder/


23. Common Weakness Enumeration(CWE) website. URL: https://cwe.mitre.org/

Index Terms

Computer Science  Security

Keywords

Software development life cycle; Static analysis; Static analysis tools; Detection Ratio; Vulnerabilities; Security; Assessment.