Evaluating and Improving Penetration Testing in Web Services

Nuno Antunes and Marco Vieira

Abstract: Developers often rely on penetration testing tools to detect vulnerabilities in web services, although frequently without really knowing their effectiveness. In fact, the lack of information on the internal state of the tested services and the complexity and variability of the responses analyzed, limits the effectiveness of such technique, highlighting the importance of evaluating and improving existing tools. The goal of this paper is to investigate if attack signatures and interface monitoring can be an effective mean to assess and improve the performance of penetration testing tools in web services environments. In practice, attacks performed by such tools are signed and the interfaces between the target application and external resources are monitored, allowing gathering additional information on existing vulnerabilities. A prototype was implemented focusing on SQL injection vulnerabilities. The experimental evaluation results clearly show that the proposed approach can be effectively used in real scenarios.