Abstract

The insecure direct object reference simply represents the flaws in the system design without the full protection mechanism for the sensitive system resources or data. It basically occurs when the web application developer provides direct access to objects in accordance with the user input. So any attacker can exploit this web vulnerability and gain access to privileged information by bypassing the authorization. The main aim of this paper is to demonstrate the real effect and the identification of the insecure direct object references and then to provide the feasible preventive solutions such that the web applications do not allow direct object references to be manipulated by attackers. The experiment of the insecure direct object referencing is carried out using the insecure J2EE web application called WebGoat and its security testing is being performed using another JAVA based tool called BURP SUITE. The experimental result shows that the access control check for gaining access to privileged information is a very simple problem but at the same time its correct implementation is a tricky task. The paper finally presents some ways to overcome this web vulnerability.
References

- C. Yang and C. Shen, Implement Web Attack Detection Engine with Snort by Using Modsecurity Core Rules&apos;, The E-Learning and Information Technology Symposium Tainan, Taiwan, 1 April, 2009.

Index Terms

Computer Science Information Science
Keywords
IDOR; Web Application; Authorization; Access control; Web exploit