ABSTRACT

Web applications have become part of our day to day life because of their user friendly nature and their advanced technology of providing internet facilities. Possibly, due to the high social impact of these web applications attackers target these in various ways. They logically enter into the system and try to execute some unintended commands or scripts which are of malicious nature. As a result it has brought lot of threats to the legitimate access. One of these threats is **Cross-Site Request Forgery (CSRF)**. CSRF is listed in **Open Web Application Security Project (OWASP)'s** [17] top ten Web Application attacks list. CSRF attack occurs in a web application due to the vulnerabilities present in the normal request response pattern of HTTP protocol [1]. An attacker execute some unintended commands by misusing such vulnerability so that an end user is forced to perform some unwanted actions on a web application in which he/she is authenticated. CSRF vulnerability is present in most of the web applications. In this project work at first, we have done extensive review on different types of web application attacks. Secondly, we analyze some of the popular existing detection and prevention techniques to handle CSRF Attacks. Finally, we propose a **profile-based verification** technique using binary search tree to verify a web document. We generate our own dataset based on our own developed application module and experimented to evaluate its performance. Our method is capable of detecting CSRF Attacks satisfactorily. This method is also an affective one based on its simplicity in implementation.