World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:8, No:05, 2014

CSRFDtool: Automated Detection and Prevention of a Reflected Cross-Site Request Forgery

Authors : Alaa A. Almarzuki, Nora A. Farraj, Aisha M. Alshiky, Omar A. Batarfi

Abstract : The number of internet users is dramatically increased every year. Most of these users are exposed to the dangers of attackers in one way or another. The reason for this lies in the presence of many weaknesses that are not known for native users. In addition, the lack of user awareness is considered as the main reason for falling into the attackers' snares. Cross Site Request Forgery (CSRF) has placed in the list of the most dangerous threats to security in OWASP Top Ten for 2013. CSRF is an attack that forces the user's browser to send or perform unwanted request or action without user awareness by exploiting a valid session between the browser and the server. When CSRF attack successes, it leads to many bad consequences. An attacker may reach private and personal information and modify it. This paper aims to detect and prevent a specific type of CSRF, called reflected CSRF. In a reflected CSRF, a malicious code could be injected by the attackers. This paper explores how CSRF Detection Extension prevents the reflected CSRF by checking browser specific information. Our evaluation shows that the proposed solution succeeds in preventing this type of attack.

Keywords : CSRF, CSRF detection extension, attackers, attacks
Conference Title : ICCNSS 2014 : International Conference on Computer Networks and Systems Security
Conference Location : Tokyo, Japan
Conference Dates : May 29-30, 2014