ABSTRACT

Web applications become a part of our day to day life because of their user friendly nature and their technology of providing facilities. Due to the high popularity attackers targeted such in various ways to violent the integrity of those systems. Attackers logically enter into the system and try to execute some unwanted commands or scripts which are unintended and are considered to be malicious in nature. As a result it has brought lots of threats of the legitimate access. One of these threats is "Cross Site Request Forgery (CSRF)". CSRF is one of the top 10 security threats reported by Open Web Application Security Project (OWASP) in 2013[2][3]. It mainly occurs, due to the vulnerability present in the normal request response pattern by HTTP protocol. An attack executes some unwanted commands by misusing such vulnerability so that an end user is forced to perform some unwanted action on web application on which she /he is authenticated. CSRF vulnerability is present in most of the web applications as reported in [2][3]. In this project, we studied various characteristics of CSRF attack and their present day detections. We also proposed a detection technique using a web-graph based matching to verify a web access. To test our proposed method we develop a small web application and generated our own data-set based on its user access. We got satisfactory result while testing the proposed method.

To implement the web-graph based matching technique we develop client-sided profile using web graph based approach to verify a legitimate user at runtime. Web graph stores behavioral access model of user for a particular application. This behavioral access model helps to identify the nature of user access dynamically – *legitimate* or *attack*. Generally we may login into an application using our login name and password, but the system or application does not know is she or he the right person or not, but there is some probability that some other person may somehow stole once login name or password. In such situation web graph helps the server to identify an user is actual or not. When an user is login into a system his behavior is dynamically compared with the behavioral access model. If it found some deviation it may terminate or may block the user according to the situation or may ask security question as the system is designed. And finally we tried to implement this methods in our self develop web application. In our attempt we capable of implement an defense CSRF attack or web attack satisfactorily. The methods are effective because of their simplicity in implementation.