ABSTRACT

Nowadays, everybody needs to handle sensitive data like online banking account details and other information related to financial transactions on the Internet. In this scenario, many Web attacks such as injection attacks are targeted on these sensitive data. Such attacks are carried out by running scripts on user’s computers that utilize a vulnerable coded client/server pages. Moreover, these attacks run malicious codes to steal personal information from the server. Further, it can easily be generated by the attacker, but very difficult to prevent by the current cross site scripting filters due to their detection accuracy. Therefore, cross site scripting attack is a challenging issue for the Internet users. Hence, it is necessary to detect and prevent the injection attacks through efficient schemes. However, most of the existing schemes lack this capability in terms of accuracy and need further improvement.

In this thesis, the new self-aware analyzing and validating the message algorithm is proposed for detecting and filtering various types of Web Service attacks. This receives request and generates the response from the dummy server page to analyze the nature of attack. The policy is created to analyze the response and forward the legitimate request to original Web Service page. The proposed injection filters have been tested with all possible attacks for verifying the robustness of filtering policies. The results obtained
from this work show that the proposed filtering policy is highly robust in refining the malicious message. The implementation and accuracy of the proposed approach has been explained through extensive testing using real-world cross-site scripting generation and analysis.

Further, the Web Services have security problems in providing authentication that need to be solved. The existing security schemes lack to defend the attacks from replay and password guessing attacks. In this research work, a new scheme for a secure authentication approach is proposed for the Web Service to enhance the security of the existing schemes. The proposed scheme has been implemented with the dynamic nonce for authenticating the user with user name and password which is embedded with WS-Security. The dynamic nonce has been implemented with the real parameters of the client/server by satisfying the conditions given in the proposed scheme. It changes the nonce for every session because it is generated from real parameters like mouse movements of the user. The system has been analyzed with all possible attacks considered in this research work. The proposed dynamic nonce based authentication scheme is suitable for system with lower configurations.
Finally, the proposed algorithms are tested against attacks and load analysis has been carried out. From the result, it is observed this system is capable of performing any type of requests. Moreover, the system takes the decision by analyzing the client’s request using self-aware message analyzing and validating algorithm.