



RESEARCH AND IMPLEMENTATION OF SECURITY FRAMEWORK FOR SMALL AND MEDIUM SIZED E-COMMERCE BASED ON SOA

Dr. ASHISH KR. LUHACH¹, RAVINDRA LUHACH²

¹Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
Email: ashishluhach@acm.org

ABSTRACT

This research paper focuses on the technical considerations for evaluating the E-commerce platform and proposed a logical security framework for small and medium sized E-commerce. The proposed logical security framework is inherited the benefits of Service Oriented Architecture (SOA) and presents an analysis of the eminent security attacks which can be prevented. The proposed logical security framework is implemented and validated on Oscommerce, an open source E-commerce. This paper also presents an analysis on the comparison between the proposed security framework and the security framework of the existing E-commerce systems such as Flipkart and Rechargeitnow. On the basis of comparison with existing security standards and validation of all the major computing attacks on the proposed security framework concludes that the proposed logical security framework helps enterprise to organize an absolute suite of amalgamated security architecture which protects E-commerce system based on SOA.

Keywords: *Service Oriented Architectures, Web Services, Encrypted Database, Security Attacks, and Legacy Systems.*

1. INTRODUCTION

With the rapid development in information and communication technology (ICT), computers became the most valuable assets to the governing body. This rapid development in ICT transforms the physical existence of the markets and E-markets introduced. Organisations start moving towards fast and dependable systems to cope up with the changing customer's demands from legacy organizations. These legacy systems have established very important tactical elements to the arrangements. The maintenance of legacy systems increased, and outweighs the benefit they generate to the organizations [1]. Legacy systems can prevent enterprises from transforming towards E-commerce, but customers are quick to take over. For instance, an organization implemented a home grown E-commerce platform 10 years ago, has already updated its legacy systems numerous times in the final ten. Updating the existing system means patching up new functionality and operability on top of already built legacy systems, now the organization ends up with a scheme which is not upgradable or even difficult to put back. These systems, tightly coupled with their legacy

systems, and it is almost impossible to shift from these legacy systems to fast and reliable systems without involving the business [2]. These legacy systems

are not compatible with modern days E-commerce systems, as today's E-commerce systems have demands of dynamic commercial enterprise applications, which are developed on the concepts of loose coupling and flexibility.

Service Oriented Architecture (SOA) is an information technology advancement in which the already existing applications of an organization employed with the various services available in a network, for example World Wide Web. These types of services which can be easily integrated with the existing one can be developed by using SOA. The main problems for developing sophisticated E-commerce systems are integration and transmission of information but SOA can ease the above mentioned problem as SOA has the feature of loose coupling. SOA has the feature of open standard protocols and excellent encapsulation this makes SOA the apt pick to employ E-commerce system [3].

2. SECURITY ANALYSIS OF SOA BASED E-COMMERCE

For accessing the E-commerce system, the users have to authenticate himself as a transaction or enterprise user. If an attacker bypasses this security mechanism of E-commerce system he will be able to gain access to the core database and product search area of E-commerce system. Figure 1 shows the generic system prototype of E-commerce system [2]. Figure 1 shows that the transaction users get access to the E-commerce platform consists of various business service components for example customer information service etc. through a web server but the enterprise user can access the business service components by directly communicating with Simple Object Access Protocol (SOAP). E-commerce system is not only used for online transactions but also can be practiced as a sequential publication of services such as banking services. Most of the E-commerce systems consist of various business services for example a famous E-commerce, Policybazar.com provide various services to their customer such as motor and health insurance. These different business services can be managed by diverse vendor or by different departments within the

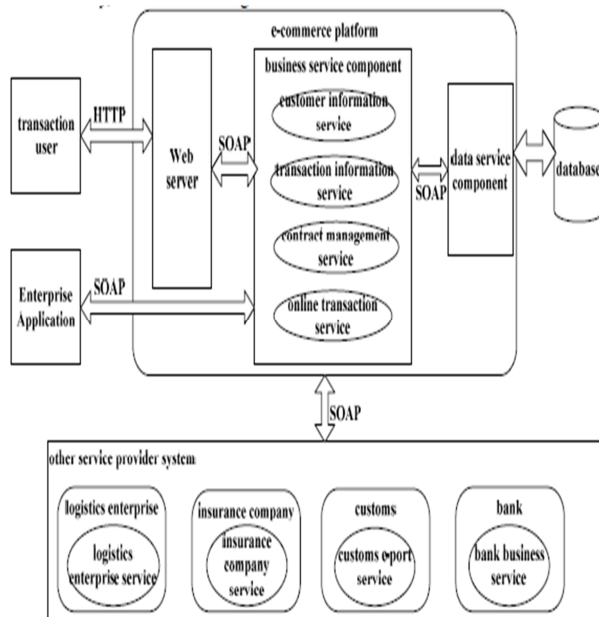


Figure 1: System Architecture of E-commerce Platform

same organisation such as Policybazar.com have different departments for the motor and health insurance which manage their own business services. The different services managed by the different departments makes an E-commerce a service oriented heterogeneous system [6][7]. On the basis of literature review conducted for this research conclude that this heterogeneous E-commerce system will have design and security issues which are certificate duplicity, Unsecure protocols, No protocols mentioned on application layer and Database encryption [8][9][10].

3. THE PROPOSED FRAMEWORK

The proposed logical security framework has the benefits of SOA designing approach. The proposed logical security framework is designed to secure the E-commerce system from know computing threats or attacks. Figure 2 shows the proposed logical security framework. In the proposed logical security framework both, the transaction and enterprise users can communicate with the E-commerce system through SOAP instead of earlier or traditional frameworks in which only the enterprise users can directly communicate with E-commerce system through SOAP. The proposed logical security framework consist of a special code or request filtering security layer know as Input Sanitization and all the transaction/enterprise users request to access the business service components of the E-commerce system are conceded through this additional security layer. Rule based plug-in is defined in the proposed logical security framework which implement an additional security layer. For efficient monitoring of the incoming and outgoing packets Intrusion detection system (IDS) and Intrusion protection system (IPS) is employed in the proposed logical security framework. With the help of Intrusion detection system (IDS) and Intrusion protection system (IPS) each and every packet is monitored and infected packets can be blocked or traced easily. Figure 2 clearly shows that the database of the E-commerce is maintained on the completely different web server named as Server 2 in the proposed logical security framework. All the business service components are maintained on different web server named as Server 1. The communication between Server 1 and Server 2 is closely monitored by the Intrusion detection system (IDS) and Intrusion protection system (IPS), which actually create additional layer of defense from attacker attempt. By placing both

business service components and database on different servers it is very easy to disconnect the database from the E-commerce to ensure the minimal loss of the sensitive information either related to customers or organization.

4. RESULTS AND COMPARISON WITH EXISTING SECURITY STANDARDS

The proposed logical security framework is validated on an open source E-commerce system, osCommerce. osCommerce is an open source E-commerce system and also provide free of cost online E-commerce solutions for various organisations. osCommerce allows organizations to arrange up their online stores without software costs or license fees. Till now, the osCommerce community provided more than 5,000 add-ons that are absolutely free of cost. osCommerce also provide customized solutions for individual clients equally well. osCommerce implemented with PHP, as web scripting language and uses MySQL as database for their server data.

started in March 2000 and has since matured to a solution that is powering many thousands of online shops around the globe. The implementation benefits which are already implemented so far for the proposed logical security framework are discussed below:

4.1 Input Sanitization

It provides an extra layer of security for the proposed logical security framework as it verifies all the incoming packets submitted by the attacker or user. If the user request consists of any special characters to bypass the security layer such as '#@123*', this extra layer of security will clean the user submitted input as '123' and forwarded to the next layer for further operation. This extra layer will resolve the issue of certificate duplicity. The highlighted text shown in figure 4.1 is a sample of infected input submitted by the attacker to bypass the security mechanism of an E-commerce system. The input sanitization layer of the proposed logical security framework will clean the infected input submitted by the user as shown in figure 4.2 (A). Figure 4.2 (B) shows the search result of an infected input "@kids#\$" on one of the famous E-commerce, Flipkart. The highlighted text in figure 4.2 (B) clearly shows the security mechanism of Flipkart doesn't sanitized the infected input and perform the search results for the same. The attackers can analysis the architecture of the security mechanism of E-

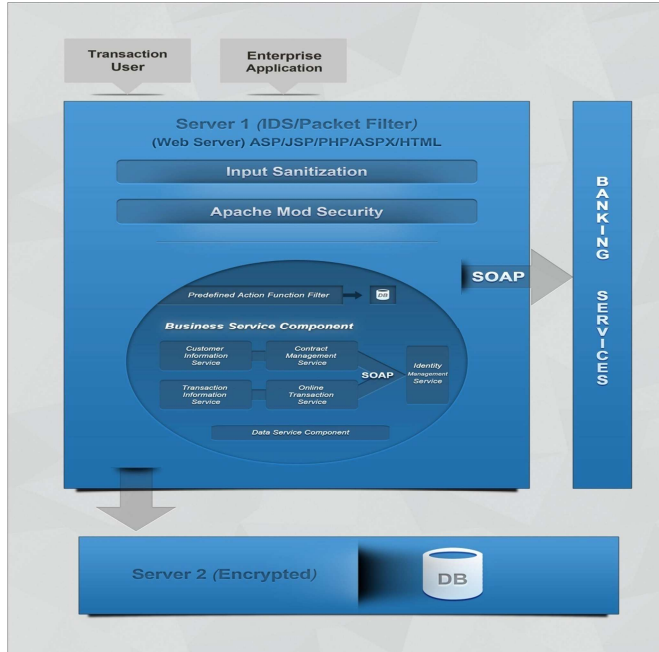


Figure 2: Proposed Logical Security Framework

The combination of PHP and MySQL allows osCommerce Online Merchant to run on whatever network server environment that supports PHP and MySQL, for example Linux, Solaris, BSD, Mac OS X, and Microsoft Windows environments. osCommerce was

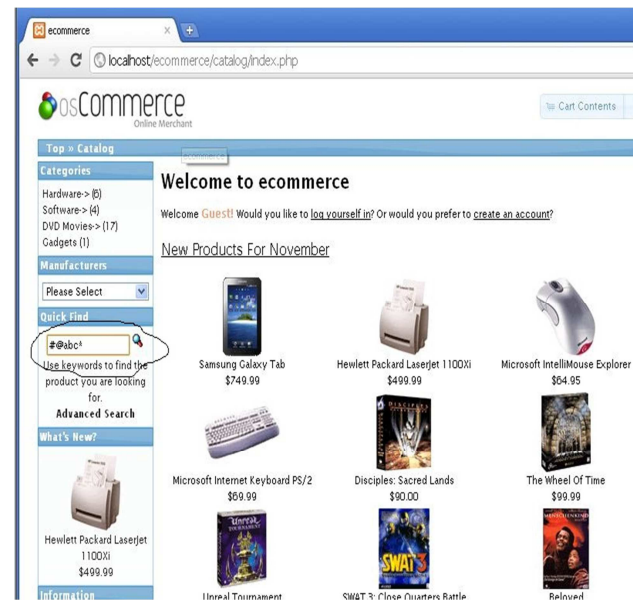


Figure 4.1 Sample Of Infected Input

commerce system by performing this type of search with infected inputs which can possible lead to successful security attacks on the E-commerce.

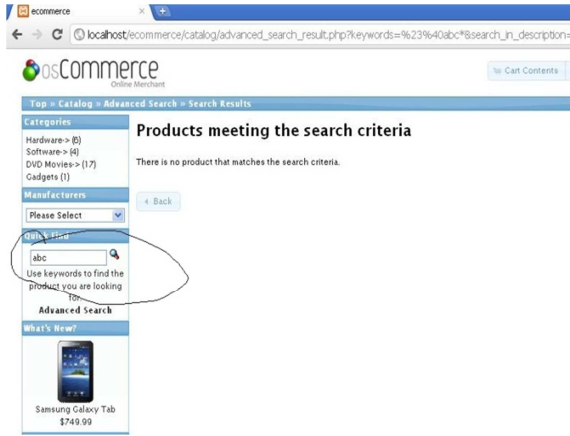
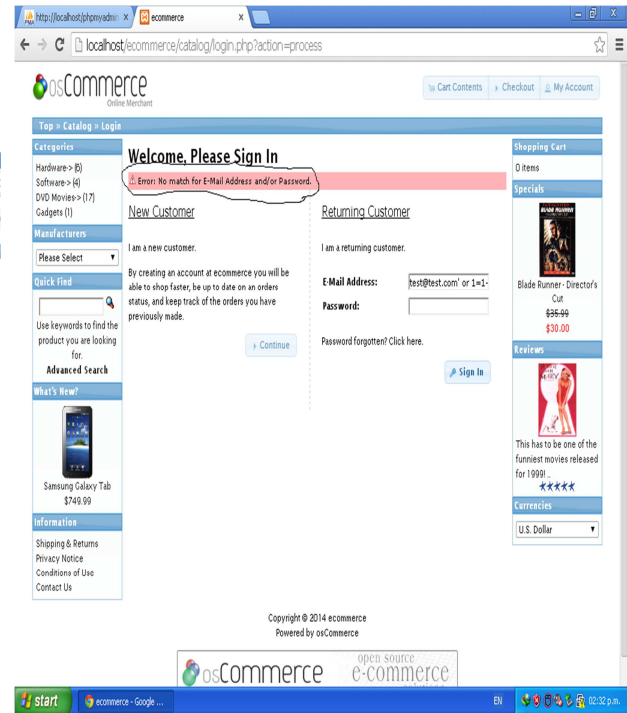


Figure 4.2(A) Sanitized Input By The Proposed Logical Security Framework.



4.2 Predefined Action Filters

These types of action filters are used to block the attacker attempt of remote code execution or SQL injection. If somehow attacker bypasses the input sanitization and able to execute his infected code then these predefined action filters block the infected code or program executed by the attacker. Figure 5.1 shows user attempt of SQL injection on customers account and Figure 5.2 (A) shows the filtering of the same for the proposed logical security framework and the web page remains the same. Figure 5.2 (B) shows a partially successful SQL injection on one of the famous E-commerce Rechargeitnow, as it displayed the error message invalid password. Somehow the attacker knows your email id for example from social media or by social engineering, and the attacker wants to access your account on E-commerce website by using your email id. Figure 5.2 (B) clearly shows that the very clear that the email id used by the attacker to access your account is valid. Now the attacker has to guess or break your password to access your account. This is a partially successful attack as the attacker input to E-commerce using your email id and arbitrary password. The E-commerce returned the error message invalid message, which makes it attacker validates one of the two user input for an E-commerce.



Figure 4.2(B) Search Results Of The Infected Input.



Figure 5.2 (A) A SQL Injection Blocked By The Proposed Security Framework

5. CONCLUSION

Throughout the context of this research work, we focused on the Service Oriented Architectures and E-commerce systems. In this research work, we have examined a comprehensive literature related to Service Oriented Architectures and E-commerce systems. The initial stage of this research focuses

on the deployment of Service Oriented Architecture, to the small and Medium Sized E-commerce system. The primary objective of this research work is to analysis the security aspects of E-commerce systems based on Service Oriented Architectures and designing a logical security

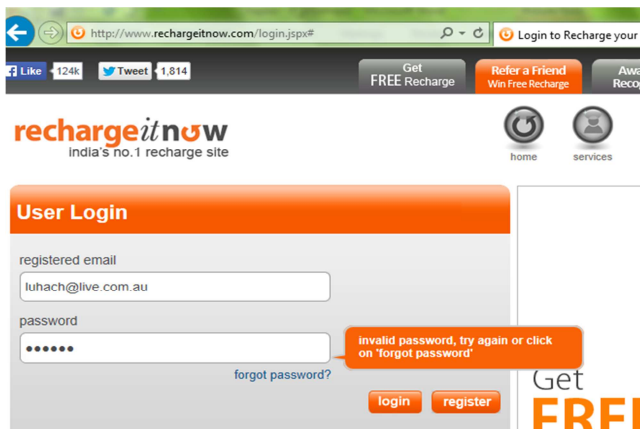


Figure 5.2 (B) Partial Successful SQL Injection

framework for the same. This research work revolves around the security aspects of small and medium sized E-commerce, as these types of organizations cannot afford the current security solutions and products or standards because they are small dot com business and do not have such infrastructure to support current security solutions. The proposed framework provides a secure E-commerce system from the major computing attacks or menaces. The framework initially implemented on an open source E-commerce system, osCommerce and proves that, it achieves all the quality attributes. For evaluating the proposed security framework all the major computing attacks are tested on. The main contribution and impact of this research is to align the benefits of SOA with E-commerce system, so that organizations can presume the combined benefits of both. The proposed security framework helps enterprise to organize an absolute suite of amalgamated security architecture which protects SOA based E-commerce.

REFERENCES

- [1] Luhach Ashish Kr., Jha C. K., Dwivedi Sanjay k. "Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA" proceeding of the International Conference on Computational Intelligence and Computing Research (ICCIC 2014), Coimbatore, Tamil Nadu, India, Pg. No. 341-346, Dec 18-20, 2014.
- [2] Maher A. Al Sheikh, Hatim A. Aboalsamh, Ahmed Albarrak, "Migration of Legacy Applications and Services to Service-Oriented Architecture (SOA)", International Conference and Workshop on Current Trends in Information Technology (CTIT-2011), Dubai, Pg No 137-142, Oct 26-27, 2011
- [3] Arsanjani A., Ghosh S., Allam A., Abdollah, T., Ganapathy S., & Holley K. (Nov 2008). "SOMA: A method for Developing Service-Oriented Solutions". Ibm Systems Journal, 47, pp 377-396.
- [4] Luhach Ashish Kr., Dwivedi Sanjay k. "Designing and Implementating a logical Security Framework for E-commerce System based on Service Oriented Architectures", International journal of



- Advanced Information Technology, Vol. -4, No.-3, Pg. No 1-10, June 2014.
- [5] Li Xiong-Yi, Research And Application Of Soa In B2b Electronic Commerce, Proceeding of the International Conference on Computer Technology and Development (ICCTD-2009), Kota Kinabalu, Malaysia, Pg. No. 649-653, Nov 15-18, 2009
- [6] Yunliang J., Xiongtao Z., Qing S., Jing F. and Ning Z., "Design of E-Government Information Management Platform Based on SOA Framework," First International Conference on Networking and Distributed Computing (ICNDC-2010), Hangzhou, pp. 165-169, Oct 21-24, 2010.
- [7] Ma H., "A Service-oriented e-Government Support Platform for Integration of Application and Data," Proceeding of the Second International Conference on Information Technology and Computer Science (ITCS), Kiev, pp. 398-401, July 24-25, 2010.
- [9] Baraka R., and Madoukh S., "A Conceptual SOA-Based Framework for e-Government Central Database," International Conference on Computer, Information and Telecommunication Systems, Amman, Jordan. May 14-16, 2012.
- [10] D.Trcek, Managing Information Systems Security and Privacy, Springer-Verlag, Berlin, 2006.
- [11] Luhach Ashish Kr., Jha C. K., Dwivedi Sanjay k, "Designing a logical Security Framework for E-commerce System based on Service Oriented Architectures", International journal of Soft Computing, Vol. -5, No.-2, Pg. No 1-10, May 2014.