International Journal on
Advanced Science
Engineering
Information Technology

Vol. 2 (2012) No. 5
ISSN: 2088-5334

Securing the Application Layer in eCommerce

Bala Musa S[#], Norita Md Norwawi [#], Mohd Hasan Selamat [*]

[#] *Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Negeri Sembilan, Malaysia*
E-mail: musa_bala@yahoo.com , norita@usim.edu.my

[*] *Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia*
E-mail: hasan@fsktm.upm.edu.my

***Abstract*— As e-commerce transaction is evolving, security is becoming a paramount issue since a great deal of credit cards, fund transfer, web shopping and public retirements are involved. Therefore, an appropriate development process is necessary for such security critical application. Also, handling security issues at early stage of software development is paramount to avoiding vulnerabilities from scaling through production environment unnoticed. This paper proposes a comprehensive security requirements and security design within the development phase of an e-commerce application as a security control to identify security flaws at early stage of web application development which might prevent re-architecture when discovered at a later stage.**

***Keywords*— Web Security; E-commerce; Software Development Process; Application Layer; Software Engineering.**

I. Introduction

A survey conducted by Danny [1] has shown that Cross-Site Scripting (XSS) attack carries about 80% of the threats in web application; SQL injection records about 62% threats while parameter tempering records about 60% of threats. This explains the fact that Cross-site Scripting, SQL Injection and parameter tempering are most important vulnerabilities to handle in web application layer as contended by SAN [2].

Previously, security experts focuses more on protecting the communication network such as building of firewalls or secure socket layers (SSL) without paying much attention on application layer where an attacker can masquerade as legitimate user to circumvent the system. This is confirmed by Stuttard [3] and Stijn [4] where they both agreed that securing the layer is a key to protecting the entire application.

Similarly, Scott and Sharp [5] affirms that there is a clear distinction between the technology which an application is implemented on (such as web servers and databases) and vulnerabilities in the web application layer. Although, putting in place secure firewalls and intelligent detection systems (IDS) provides security only at the network level leaving the web application layer vulnerable to attacks.

Therefore, we present in this paper a preemptive approach to security by building checks at requirement and design phase of software development process in order to identify any security flaws at the early stage which might prevent re-architecture when discovered at a later stage.

II. Relevant Work

Future works such as Huang [6] have created lattice-based static analysis algorithm approach to mitigate an immediate vulnerabilities emanating during coding stage of web application development. It provided a sound verification and reduces false positives.

Similarly, Keramati [7] uses an efficient activity integration algorithm with some parameters of Agility reduction tolerance to restrain the nature of organization agile process. The approach begins by extracting security activities and defining degree of agility.

Furthermore, in an attempt to provide an early thought on security during the development of a web application, Meladath [8] uses use cases to identify security threats and security requirements which he referred as a beginner's sensitization framework.

Although, other works such as Ge [9] combined security approach like risk analysis with feature driven development (FDD) to address security in web application layer, the methodology emphasis on the design and building phase [10].

But the most significant to e-commerce security development process is the work proposed by Sengupta [11] which is referred to as e-commerce security. They investigated the technology and requirements that are necessary to mitigate vulnerabilities in e-commerce application.

Therefore, our approach emphasis more on the requirement and design phase since most of the vulnerabilities that are not properly handle at this phases scale to other phases unnoticed.

A. Security Approaches

Practitioners and researchers have developed processes to deal with threats and vulnerabilities in web application. Some of these processes include:

1) Threat Modeling

This is an important process that maps out the likely areas of attacks or vulnerabilities that might emerge as a result of a software development process. It provides detail information of the likely risk that could circumvent an application. In addition, threat modeling tends to identify as earlier as possible the possible risk to an application so that it could be handled before production environment. Previous works such as [1] uses threat modeling known as STRIDE (Spoofing, Tempering, Repudiation, Information Disclosure, Denial of Services and Elevation) to design a fuzzy logic-based technique with fuzzy input variables, while Stijn [4] uses STRIDE as on WE Rock 24/7 to obtain a threat model document. Olzak [12] proposes a high level methodology for threat model in order to produce a blue-print document that benefits security analysts.

2) SQL Injection Detection

This security approach is employed to detect SQL injection attacks by observing output causing the injection. The web application is subjected to black box testing that does not require original program code. Therefore, the report of likely areas of vulnerabilities is generated which specifically describes the injection. The approach begins by scanning through the web application for a HTML forms which primarily allows for data entry by a user and thus serve as a medium for injection [13].

3) Cross-Site Scripting

This approach is similar to the SQL injection detection where a crawler is used to map out links in web application that might contain malicious codes while other links that are not malicious are similarly mapped in the process.

B. Security requirements

Security models generally comprises of requirement, design, development, testing and implementation phases [14]. Therefore, building security at early stage of system development ensures that applications are secured to certain degree. Unlike business requirements, security requirements needs the collaboration of all stake holders such as security team, system analysts, database administrators, legal practitioners, business representatives and other policy makers. Security requirements should clearly state the function, processes, transaction and data that need to be protected in the organization. Other task that needs to be secured is the internal/external access and authorization. A use and misuse case also ensures that services and features that need to be protected are also gathered to have a complete requirement specification.

The use case shows how legitimate users interact with the modules in the application. On the contrary, the abuse case shows how an illegitimate user can circumvent the system at various stages. The abuse case aid the building of security features around the areas of vulnerabilities. Most interesting about the abuse cases is that it identifies the shortcomings that can trigger security breach in an event the system is deployed to production environment. Therefore, a comprehensive abuse case implies a tighter security control in the application.

C. Security Design

The requirements gathered at the initial stage forms the bases for security design while considering the inherent vulnerabilities and features of what the application is meant for. The design further captures the complete breakdown of functions, processes and modules of the entire application. Therefore, for security purposes, the perceived vulnerabilities must be handled and analyzed in order to build an optimal security solution. The security policy which must agree with the master policy of the organization is also an important aspect to deal with.

III. Propose Security Requirement

This section presents the proposed security requirements which involve identifying important security threats at very beginning to disallow vulnerabilities scaling through the subsequent phase of development. Therefore to capture a broad range of security requirements, all stake holders including business representative, security experts, system analysts, development team etc, need to collaborate. By so doing, developers can gain insight on company's policies and regulations, while the business representative will be briefed on the risk involved when an attacker circumvents the system of the organization. This sort of deliberation may trigger an informed policy revision or an entirely new policy.

a. Definition of detail physical and intellectual properties to be protected in an e-commerce environment. This includes the web servers hosting the e-commerce, the client components that receive the services from the other end and the linking channel that transmits data between client and servers. Therefore the security of the assets has to be detailed in line with the company security policy.
   - Web servers are the storage for e-commerce transaction. They supply feedback to the client request coming from web browser in HTTP using web server software. Therefore a vulnerability assessment of all components is necessary since exploiting a component by an unauthorized user can pave way for acquiring sensitive information which can be very devastating to the company.
   - Client components such as active contents that facilitates online shopping by clients via virtual shopping cart. The active content forms include Java Applets, VB Script, Active X controls etc. therefore, details of how to protect these components is paramount in an e-commerce environment where malicious codes or script can be embedded to reveal a great deal credit card numbers or users password.
   - Linking channels connects the client side with the server side. Therefore an enforcement of policy

such as confidentiality, integrity etc will guaranty that messages that are transmitted back and front between client and server is not tampered with.

b. Detail processes include activities that needs to be performed, security issues that needs to be put in place and policies that needs to be enforced. The following activities are carried out in this process:
   - Authorization. Users has to be checked or verified with the internal rules to ensure that only authorized individual can carry out certain operations. Also incoming data has to be validated.
   - Privacy of data. Users' information must be made private using encryption to disallow attackers from gaining access or standing in the middle.
   - Define use and misuse case for functionality guaranty. In this case, the functionalities of the system must be developed while abuse or misuse cases should also be derived. The use case spells out how the system works under normal circumstance while the misuse or abuse case is the abnormal circumstance of how attacker can gain access or circumvent the system. The formulation of the misuse case will aid further adjustment of processes and functions.

IV. Proposed Security Design

The design stage of software development process generally involves designing an abstraction diagrams such as transition, class, components and sequence. The class diagram will show how objects will interact with the system, while sequence diagram will show the interaction of the objects to achieving the entire function of the system. Therefore for the purpose of ensuring e-commerce application security, security levels should be given utmost consideration. Detail abstraction of security design in each representation is proposed, a refactoring and revision of design at each level and a risk assessment for vulnerability.

V. Case Study

We examine in this proposal, a shopping cart activity of an online bookshop where a user or customer browses the home page in search of a book either by using a keyword or just simply checking the books available in a specific domain. It is expected that he uses a login form to add the book of his choice to his cart and hence places an order. The requirement gathering in this case should include comprise of both business representative and technical team. Also the same technique and tools used to capture business requirement should also be used for security requirement as well.

Therefore, since the major concern is the security of e-commerce application, we stick to the following requirements:

a. Customer search for books on the home page using a keywords

b. The customer is expected to login and provide some basic information in order to add his choice of books to his cart and make a purchase

c. Customer makes an order

In defining the requirement for this scenario, we begin with detail physical and intellectual property protection which includes:

- Active content protection
- Confidentiality of client-to-server communication
- Defenses against attacks such as spoofing, defacement etc
- Defenses against any database attack

We further detail out the data processes to include

- Search books
- View cart
- Add to cart
- Delete from cart

Our Use Cases will therefore be defined in simple terms as:

- Customer search books using keywords
- Customer login
- Customer view his cart list
- Customer adds or delete book item from his cart

Similarly, a Misuse case is also derived as:

- At login, an attacker can brute force password
- Attacker can craft a malicious code, attempt to reveal stored cookies, or tamper with parameter during view cart, add cart or delete cart

At the design stage, sequence, class, and use case diagrams are abstracted from the requirements. Figure 1 illustrates the use case diagram.

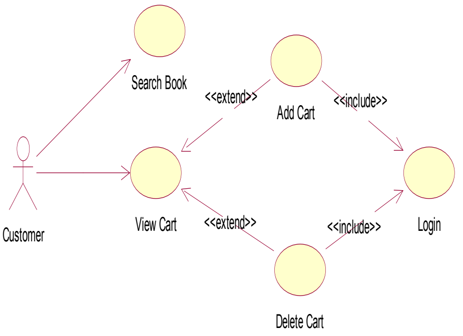

Figure 1 Use case diagram for Online Bookstore

The Misuse case in this context is illustrated in Figure 2. The attacker can use different mechanism to circumvent the system during customer transmission of his details to the server.

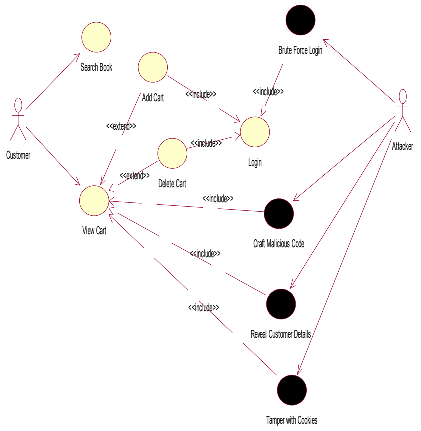

Figure 2 Misuse case diagram for Shopping Cart Activity

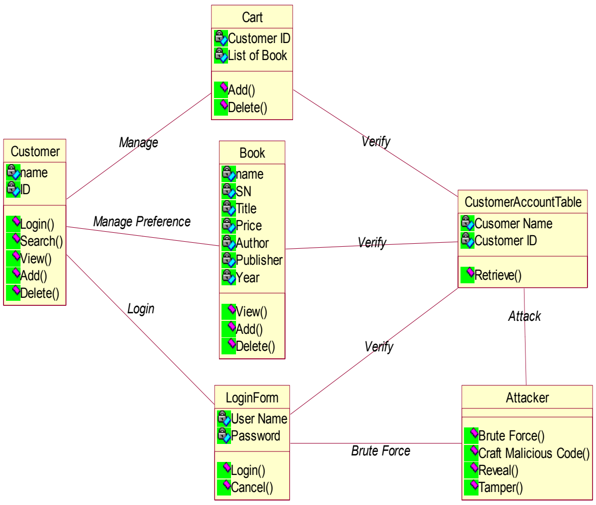

Figure 3 Class diagram for customer and attacker

The respective sequence diagram for search, view and add book item to cart is shown in Fig 4, Fig 5 and Fig 6 respectively

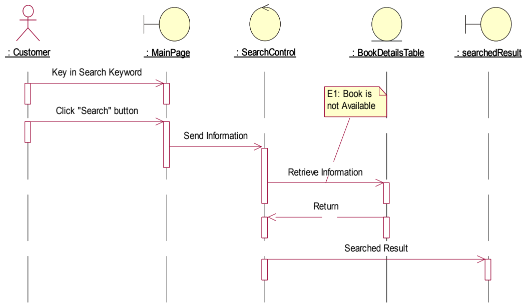

Figure 4 Sequence diagram for search book

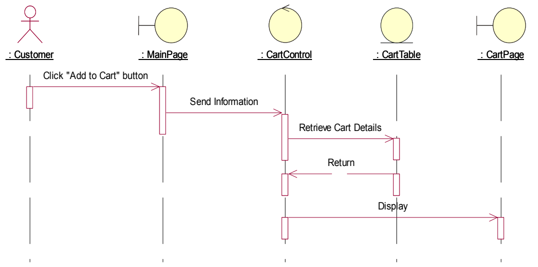

Figure 5 Sequence diagram for view cart

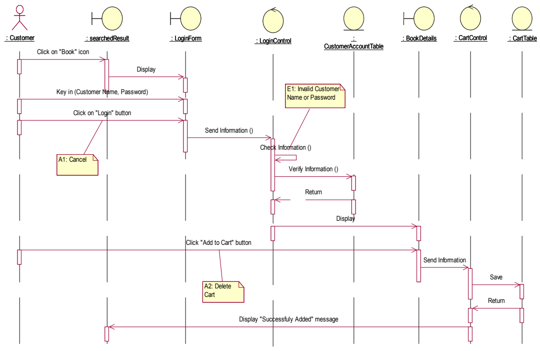

Figure 6 Sequence diagram for Add cart

VI. Conclusions and Future Work

This approach tightens security at the very beginning of an e-commerce application development process. It ensures that security threats are identified and filtered at early stage, which in essence prevents it from scaling through production environment. The approach when implemented will trigger policy review in the part of business representatives and review of defenses on the part of development team.

Further research will focus on coding and implementation stages of the process with an in-depth comparison with other processes in the domain.

Acknowledgment

Our special thanks go to the Dean School of Post Graduate Studies (Prof. Dr. Bachok M. Tiab) for his immense guidance and to all our reviewers who made it possible to accomplish this research.

References

[1] A. Danny, “Managing a growing threat: an executive’s guide to Web application security,” in Web application security Executive brief, NY, USA, 2007, pp. 4.

[2] Sysadmin Audit Network Security SANS/FBI, “Top Cyber Security Risk,” in SPI Dynamics Inc, 2009.

[3] D. Stuttard, and M. Pinto, The web application hacker's handbook : discovering and exploiting security flaws, Wiley Pub., Indianapolis, IN, 2008.

[4] V.K. Stijn, “Threat Model for Web Application Using STRIDE Model,” in Information System, Royal Halloway University London, 2004, pp. 80.

[5] D. Scott, R. Sharp. "Developing Secure Web Applications." IEEE Internet Computing vol. 6, pp. 38-45, 2002.

[6] Y.W. Huang, F. Yu, C. Hang, C.H. Tsai, D.T. Lee, and S.Y. Kuo, “Securing web application code by static analysis and runtime protection,” in Proceedings of the 13th international conference on World Wide Web, ACM, New York, NY, USA, 2004, pp. 40-52.

[7] H. Keramati, and S.H. M. Hosseinabadi, “Integrating software development security activities with agile methodologies,” in Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications, IEEE Computer Society, 2008, pp. 749-754.

[8] D. Meledath, “Secure Software Development Using Use Cases and Misuse Cases,” in Information Systems, 2006.

[9] X. Ge, R.F. Paige, F.A.C. Polack, H. Chivers, and P.J. Brooke, “Agile development of secure web applications,” in Proceedings of the 6th international conference on Web engineering, ACM, Palo Alto, California, USA, 2006, pp. 305-312.

[10] S.R. Palmer, and M. Felsing, “A Practical Guide to Feature-Driven Development,” Pearson Education, 2001.

[11] A. Sengupta, C. Mazumdar, and M. Barik, “e-Commerce security — A life cycle approach,” Sadhana vol.30, pp. 119-140, 2005.

[12] Olzak, T. "A practical approach to threat modeling," 2006.

[13] Y.W. Huang, S.K. Huang, T.P. Lin, and C.H. Tsai, “Web application security assessment by fault injection and behavior monitoring,”in Proceedings of the 12th international conference on World Wide Web, ACM, Budapest, Hungary, 2003, pp. 148-159.

[14] M.S. Bala, M.N. Norita, and S. Mohd Hasan, “Secure E-commerce Web Development Framework,” in Information Technology Journal, DOI: 1812-5638, 2011.