Research Article

Review of e-Commerce Security Challenges

[1]Kalpana Dhende, [2]Dr. Shweta Meshram
Department of Master in computer Application
MES's Institute of Management and career courses, Pune, India

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract*:* e-Commerce means nothing but the exchange of goods and services over the Internet.
This paper gives a way for e-commerce security so as to improve confidence in customer. Web security has become most important issue now a day. Online payment system now a day most of time people uses online payment system for payment, so all the manual payment is replaced by online payment system. The main objective of this paper is to know the views of consumers towards the security aspects of e-commerce technology. This paper gives the idea about the perception and awareness of security from the consumers' views. The paper also examines the measures that can be taken so that the views of users can be changed to adopt this new on-line system. This new security challenges are the results of the use of the new technology and communication medium, and the flow of information from organization to organization, from organization to consumers, and also within the organization.

***Index Terms*—**e-Commerce, Security, Threats and Vulnerabilities, SSL, Firewall, viruses. E-commerce security, e-business security challenges.

I. INTRODUCTION

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider Information Security framework. E-commerce security has its own shades and is one of the highest security components that affect the end user through their daily payment interaction with business. e- Commerce environments composed of front-end web pages, back-end databases, web servers, and internal network infrastructure. The vulnerable areas of an e-commerce system must be identified and resolved to reduce the risk to security.

II. SECURITY OVERVIEW

In an e-Commerce system security hardware, software, and environment are the main important and vulnerable points. Hardware security includes devices used in running the e-Commerce website like web servers, database servers and client's computer.
The Properly configured firewall system can be helpful to protect the network. Any software used in running the e-Commerce system such as the operating system, web server software, database software and web browser are part of securing software .to protect the network from various threats, operating system should be configured properly. Software and routinely released patches should be regularly updated to fix security holes. The website development should provide protection against attacks like hidden-field manipulation, tampering, buffer overflow, and cross-site scripting. Cryptography algorithm can be used to protect confidential data which can be entered by end user.

III. Security Threats

3.1 Online Credit Card Fraud

Credit card fraud main cause is the usage of credit card over the Internet. Credit card to a certain extent portrays the following threats:

MasterCard misrepresentation fundamental driver is the utilization of Visa over the Internet. Charge card to a limited degree depicts the accompanying dangers:

presently a day's Visa misrepresentation is most normal approach to take cash. programmer can hack charge card number and can utilize it for individual use. The lone safety effort on charge card buys is the mark on the receipt however that can without much of a stretch be produced. The greater part of time individuals neglect to gather their duplicate of cards subsequent to taking care of bills of cafés. These receipts are containing individuals' MasterCard number and people signature for anybody to see and utilize. Just by this data somebody can buy online things. Also, the approved individual will not notification this until the individual gets month to month proclamation so Make sure

the site is trusted and secure when doing shopping on the web. With the assistance of phishing procedures, a few programmers may take a few to get back some composure of your Visa number.

3.2 Confidentiality

Secrecy is one of the significant measure which can be broken from numerous points of view. Assailants don't require refined comprehension of the PCs and Internet to break an organization's PC. passwords and charge card numbers and extortion guidance guides are accessible in Internet visit rooms. Other than this, many web worker have PCs that runs different workers other than the web worker. Model is the FTP worker.

3.3Authentication

Space Name System (DNS) satirizing is additionally conceivable with inappropriately set authorizations. In DNS parodying, If the two pages seem to be indistinguishable, even judicious clients can be effortlessly cheated and the company‟s notoriety harmed.

3.4 Vulnerabilities

Security penetrates happens time after time when safety efforts are by passed. Classified subtleties can be shared like sharing passwords or OTP via telephone or tossing security manuals without destroying can make issues on the off chance that it falls in some unacceptable hand.

By having tight access control one can have control on framework security. That is by giving the Workers access just to their work capacities and not more than that.

3.5 Security System Design

Great security configuration incorporates great general control, appropriate isolation of obligations, plainly outlined lines of power, inward review, great documentation, legitimate approval, interior review and endorsement for the two exchanges and program changes. With every one of these actions set up, we ought to deliberately concentrate on the anticipation, discovery and amendment of safety penetrates.

IV Main Security Solutions

Online business requires another kind of safety. conventional security frameworks are intended to keep individuals out and limit admittance to significant data and registering assets. nonetheless, web based business requires security frameworks that give approved untouchables admittance to restricted organization assets and applications, regardless of whether they're online installment frameworks, stock information, or the capacity to do exchanges with the assistance of Internet. As the innovation arises, the accompanying procedures have been created to straighten out security. Once more, the issue here is the means by which far the purchasers know about these innovations. A couple of innovation techniques to conquer the Internet security dangers are recorded underneath.

4.1 Encryption

Touchy data, for example, charge card subtleties can be secured by encryption, that should be possible with the utilization of mystery codes. The objective of encryption is to make lucid content into non decipherable arrangement so it makes inconceivable for a programmer who acquires the code text (ambiguous type of the message in the wake of being encoded) as it goes through the organization, to recuperate the first message. Encryption is the change of significant data in any structure into a structure that must be delivered clear with the assistance of decoding key. There are two fundamental sorts of encryption in like manner use today – symmetric, or private key frameworks and deviated or public key frameworks. In a symmetric key framework, a similar key is utilized to encode and decode the plaintext. The key is known as a private key and should be shared by the sender and recipient of the content. Public-key encryption utilizes two firmly related keys. One key is utilized to scramble the message, and the other key is utilized to unscramble the message. The public key can be spread the word about for different gatherings or we can say to recipient, and can be circulated uninhibitedly. The private key should be kept secret, and should be known distinctly to its approved proprietor. The two keys, in any case, should be secured against the smallest change, or the component won't work. Model is RSA calculation

4.2 Digital Signature

A computerized mark is a numerical method used to approve the realness and honesty of a message, programming or advanced record. It's what might be compared to a transcribed mark or stepped seal, yet it offers undeniably more intrinsic security. A computerized mark is expected to tackle the issue of altering and pantomime in advanced correspondences.

Advanced marks can give proof of starting point, personality and status of electronic archives, exchanges or computerized messages. Endorsers can likewise utilize them to recognize educated assent.
In numerous nations, including the United States, advanced marks are viewed as legitimately restricting similarly as conventional written by hand record marks.

4.3 Digital Certificate

Validation is additionally fortified by the utilization of computerized authentications. Advanced declarations confirm that the holder of a public and private key is who they guarantee to be. Outsiders called endorsement specialists (CA) issue advanced authentications. Most declarations follow the Internet Engineering Task Force's (IETF) X.509 testament standard. Under rendition 3.0 of this norm, an endorsement contains things, for example, the subject's name (proprietor of the private key), legitimacy period, subject's public key data and a marked hash of the testament information (for example hashed substance of the endorsement endorsed with the CA‟s private key). Endorsements are utilized to validate Web locales (website authentications), people (individual testaments) and programming organizations (programming distributer declarations) VeriSign issues three classes of authentications. Class 1 checks that an email really comes from the user's address. Class 2 checks the user's character against a business credit information base. Class 3 necessities authenticated records. Organizations like Microsoft offer frameworks that permit organizations to give their own private, in-house authentications. These can be utilized to recognize clients on their own organizations

4.4 Cross-site script (XSS)

Cross-webpage scripting (referred to likewise as XSS) is a sort of assault focused on web application clients. Assailant infuses customer side code (regularly a JavaScript) into weak web application so that the content is run on client's programs visiting weak page. Envision that you've assemble a web application permitting your clients to send private messages to one another. One of the clients discovers that you don't encode messages, so it is feasible to send unadulterated HTML or JavaScript code to other individual. The client chooses to send this message to his pal:

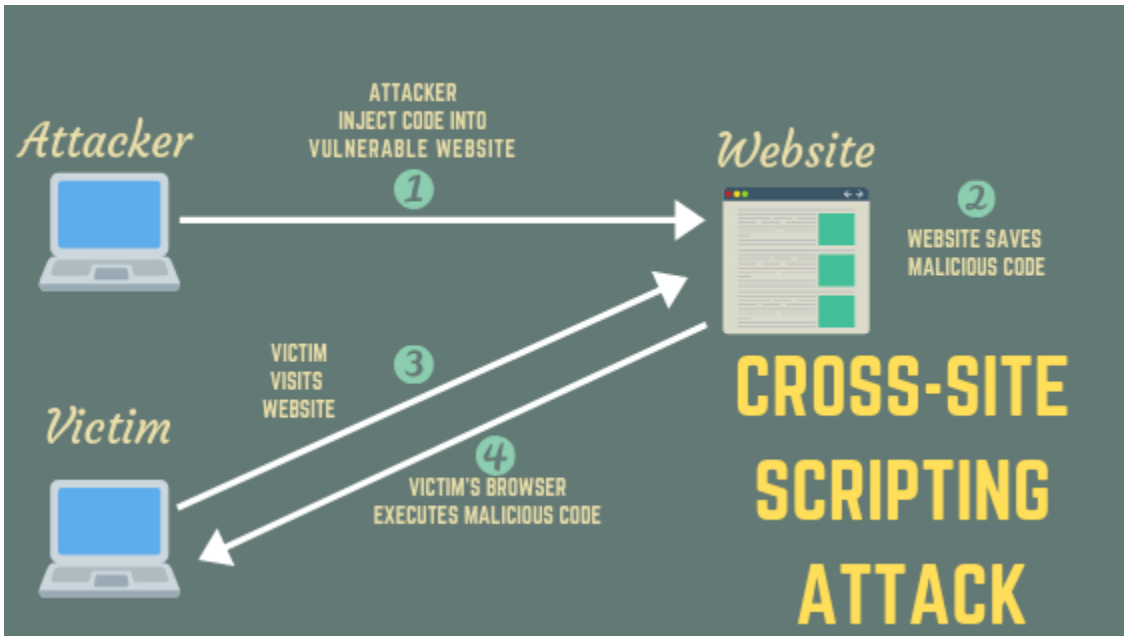

Figure 4.4 Cross site scripting

4.5. Personal Firewalls

While interfacing our PC to an organization, it gets helpless against assault. An individual firewall ensures our PC from external assailant by restricting the sorts of traffic started by and coordinated to our PC. The aggressor can check the hard drive to recognize any put away private subtleties or information. Numerous PCs are tainted by spyware or some likeness thereof. Most are 'innocuous', however an expanding number pass into infections that will take and send secret data,

4.6. Secure Socket Layer (SSL)

Secure Socket Layer is a convention that scrambles information between the customer's PC and the site's worker. At the point when a Secure attachment Layer-ensured page is mentioned, the program distinguishes that the worker as a confided in substance and starts a handshake to pass encryption key data to and fro. Presently, on ensuing solicitations to the worker, the data streaming to and fro is scrambled so a programmer sniffing the organization can't peruse the substance. SSL permits moving information in a scrambled structure. All data that a client should keep hidden ought to be communicated through SSL. Such data should incorporate Mastercard number and related data, and may, contingent upon the sort of business, incorporate client's name, address, and the rundown of items that the client is purchasing. It ought to likewise incorporate the client's secret word and request ID.

4.7. Web Server Firewall

A web worker or web application firewall, either an equipment machine or programming arrangement, is set in the middle of the customer end point and the web application. Web application firewalls secure cardholder information since all web layer traffic is investigated searching for traffic A firewall resembles the channel encompassing a palace. The external firewall has ports open that permit ingoing and active HTTP demands. This permits the customer program to speak with the worker.

4.8. Password policies

We may decide to have various strategies for customers versus our inside clients. For instance, we may pick to lockout a director after 3 fizzled login endeavors rather than 6. These secret phrase arrangements ensure against assaults that endeavor to figure the client's secret key. They guarantee that passwords are adequately sufficient so they can't be effectively speculated.

4.9. Installing Recent Patches

Programming bugs and weaknesses can be recognized each day. Despite the fact that a significant number of them are found by security specialists, instead of programmers, they may in any case be abused by programmers once they turned into a public information. This is the motivation behind why it is critical to introduce all product fixes when they become accessible.

5.0. Intrusion Detection and Audits of Security Logs

Security logs are very important to follow the client record. For model, if an individual compose secret phrase wrong, and every one of the 6 time if the individual is composing incorrect password then ,that people account gets locked. This occasion ought to likewise be signed in the system, this should be possible by sending email to the administrator. We can likewise have logged or record the unapproved admittance to the framework.

V. CONCLUSIONS

Current technology allows to design secure site. It is important to always keep in mind that whatever are the security measures are described and explained do afford a good sense of protection, we should always use and follows above security ensures in order to have safe online shopping or online payment.

References

1. Foresight (1998), “E-commerce Sets New Rules,” *Systems Relationship Marketing,* on behalf of DatatecLtd, Vol. 1 No. 3, November.
2. Morgan, C. (1999), Protecting Your Website Against Credit Card Fraud. *Computerworld,* , p.71.
3. Young, J., Spies like us. *Forbes*, June 3, 1996, pp. 70-92
4. Chokani.S and Ford, W., Internet Public Key Infrastructure Certificate Policy and Certification practices Statement Framework, Internet Draft, September, 1997
5. Greenwich, Conn.-IVANS (Insurance Value Added Network Services) source :www.ivans.com
6. McKeefry www.ebnonline.com/supplements/ extras/story/OEG20000406S0006

7. Chew, K.W., (2003) "*To Determine the Readiness of Business Entities and Consumers for A Successful Implementation of Electronic Commerce in Malaysia*" End-of –Project Report submitted to the Ministry of Science, Technology and the Environment, Malaysia.

8. Julie,B(1997)., http://disc.cba.uh.edu/~rhirsch/fall96/barba.htm

9. Portz *et al* (2000) http://uwstudentfpweb.uwyo.edu/J/JP/WebTrust.html Ramsey and eMarketer - www.newsfactor.com/perl/story/6530.html

10. Chadwick,S.A., http://chadwick.jlmc.iastate.edu/

11. Electronic Commerce, Second Annual Edition, Gary P. Scheneider and James T. Perry, p3

12. Bonafield, C.H., (1998), Cashing In on E-Commerce. Network Computing.

13. Miyazaki, Anthony D. and Fernandez, A., (2000), "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy and Marketing*, 19 (spring), 54-61.

14. Kalakota, R and. Whinston, A. B. (1997). *Electronic Commerce: A Manager's Guide.* Addison Wesley.

15. Turban, E., King, D., Lee, J., Warkentin, M. and Chung, H.M. (2002*) Electronic Commerce: A Managerial Perspective 2002*, Prentice Hall, USA.

16. E-Commerce and Security, http://www.it.uu.se/edu/course/homepage/ehandel/vt08/

17. A. Kahate, Cryptography and Network security, Tata McGraw Hill Education Private Limited, 2nd edition, 2008

18. SQL Injection, http://en.wikipedia.org/wiki/SQL_injection

19. Security Response, http://securityresponse.symantec.com/avcenter/refa.html

20. C. V. Berghe, J. Riordan, and F. Piessens, *A Vulnerability Taxonomy Methodology applied to Web Services*, IBM Zurich Research Laboratory,
2005.

21. R. Ganesan, M. Gobi, and K. Vivekanandan, \A novel digital envelope approach for a secure e- commerce channel," *InternationalJournal of Network Security*, 2010.

22. M. Hung, and Y. Zou, \A Framework for Exacting Work flows from E-Commerce Systems," *Proceedings of Software Technology and Engineering Practice*, pp. 43{46, 2005.

23. F. Nabi, \Secure business application logic for ecommerce systems," *Computers & Security*, pp. 208{217, 2005.

24. Qi XIE, Lihong ZHAO. Research and realization of web services security. *Computer Engineering and Design*,2007,

25. Zhu Lingxi. *E-Bunsiness Security. BeiJing*. Beijing Jiaotong University. 2006.

26. W3C Working Group Note, "Web services architecture", http://www.w3c.org/TR/ws-arch, 2004.

27. Apache Software Foundation, "Filters - Apache HTTP Server," http://httpd.apache.org/docs-2.1 /filter.html, Nov.2004.

28. E-commerce http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.Html

29. Ravi Kalakota, Andrew B. Whinston. Electronic Commerce: A Manager's Guide, Addison-Wesley, ISBN: 0-201-88067-9

30. Critical Threats e-Commerce hosting, http://www.plaveb.com/blog/3-critical-threats-toecommerce- hosting

31. Threats e-Commerce Server,http://www.technologyexecutivesclub.com/Arti cles/security/artThreatsto Ecommerce Servers.php

32. E-Commerce site security, http://www.applicure.com/solutions/eco

33. e-commerce-security H. S. Yoon and L. G. Occeña, "Influencing factors of trust in consumer-to-consumer electronic commerce with gender and age," *International Journal of Information Management,* vol. 35, pp. 352-363, 2015.

34. UNCTAD, "Information Economy Report 2015-Unlocking the Potential of E-commerce for Developing Countries," 2015.

35. OECD, *https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm (accessed 20 April 2016),* 2011.

36. S. Kurnia, J. Choudrie, R. M. Mahbubur, and B. Alzougool, "E-commerce technology adoption: A Malaysian grocery SME retail sector study," *Journal of Business Research,* vol. 68, pp. 1906-1918, 2015.

37. S. Chatterjee, "Security and privacy issues in E-Commerce: A proposed guidelines to mitigate the risk,"