ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Review of e-Commerce Security Challenges

Jarnail Singh
Dept. of Computer Science & Engineering, Laxmi Devi Institute of Engineering & Technology, Alwar, Rajasthan, India

Abstract*:* e-Commerce refers to the exchange of goods and services over the Internet. The shopping through e-commerce has penetrated all segments of goods ranging from groceries to electronic goods and even vehicles. Rapid growth in mobile computing and communication technologies has facilitated popularity of e-commerce. The main impediment in growth of e-commerce is cyber fraud and identity theft. Hackers are people who carry out the cyber crime. Hence, poor security on e-Commerce web servers and in users computers is core issue to be resolved for rapid growth of e-commerce. This paper provides directions for e-commerce security so as to improve customer confidence in e-commerce shopping.

Keywords: e-Commerce, Security, Threats and Vulnerabilities, SQL Injection, DDoS, SSL, Firewall, Session Hijack, Viruses.

I. INTRODUCTION

Online shopping or exchange of goods or services over the Internet is as old as Internet. It is gaining popularity and has tremendous scope for growth as computing devices and communication technologies are making rapid advancements and becoming cost effective day by day. Mobile computing has enormous potential to make e-commerce a most popular mode of shopping. Entrepreneurs want to provide quality of service to customers and maintain customer's trust by ensuring high availability, sufficient capacity, and satisfactory performance for their e- Commerce Web systems. Security is main concern of customer that is hampering the rapid growth of e-commerce transactions. Security issues such as destruction, disclosure, and modification of data, denial of service, fraud, waste, and or abuse of network resources must be resolved in order to build trust of customers in the e-commerce. e- Commerce environments consist 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 of security threats.

II. SECURITY OVERVIEW

In a e-Commerce system security hardware, software, and environment are the main critical and vulnerable points. Hardware security includes any devices used in running the e-Commerce website like network devices, web servers, database servers and client's computer. Securing the network with a properly configured firewall device that is only allowing ports needed for accessing the e-Commerce website is an essential part of network security. The web server and database server should be isolated from other networks using a network DMZ to reduce possible intrusion from compromised computers on other networks behind the firewall. A DMZ or demilitarized zone is a separate network added between a protected network and an external network, in order to provide an additional layer of security [1].
Any software used in running the e-Commerce system such as the operating system, web server software (IIS, Apache) and database software and web browser are part of software security . The operating system is the main component of security that should be configured properly so as to take care of security vulnerability. Software and routinely released patches should be regularly updated to fix holes in security. The website development itself should ensure protection against attacks like cookie poisoning, hidden-field manipulation, parameter tampering, buffer overflow, and cross-site scripting. Website pages, where confidential information is being entered, should be secured with strong cryptography algorithm.

Environment security refers to secure physical access to network and server devices by using manual guard, CCTV, locks, or other methods. Network, server, and software access credentials should be highly complex and well guarded.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

If any staff member leaves the company, all access privileges for that person should be immediately removed. Staff members should also be trained against cyber frauds in which sensitive information may be given to attackers posing as a trustworthy person over the phone or email or through forge websites.

The secure an e-Commerce website is a dynamic process where new threats crop-up every day. To retain customer's trust in e-commerce systems, a proper planning should be done to stay protected against possible security threats. To build a secure e-commerce application, following five security features must be included

Authentication: This mechanism helps establish proof of identities. This process ensures that the origin of a electronic message or document is correctly identified.

Integrity: when the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of message is lost. Integrity of message should be intact i.e. message should not be tempered in transit.

Non repudiation: There are situations where a user sends a message and later on refuses that he/she had sent that message. Non repudiation does not allow the sender of a message to refute the claim of not sending that message.

Access control: The principle of access control determines who should be able to access what.

Availability: The principle of availability states that resource should be available to authorized parties at all times.

Cyber crime cases in the country registered under the IT Act last year rose by about 61 per cent to 2,876 with Maharashtra recording the most number of cases. The country had witnessed 1,791 cases registered under the Information Technology (IT) Act in 2011. "As per the cyber crime data maintained by National Crime Records Bureau (NCRB), a total of 288, 420, 966, 1,791 and 2,876 cyber crime cases were registered under IT Act during 2008, 2009, 2010, 2011 and 2012, respectively,". Maharashtra registered a total of 471 cases in 2012 followed by Andhra Pradesh (429), Karnataka (412), Kerala (269) and Uttar Pradesh (205) under the IT Act. "To address the growing threat of cyber crimes/incidents in the country, government has issued an advisory to state governments and union territory administrations advising them to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes[4].

A. Client side Security

The user's privacy and integrity of information should be protected at client side. Antivirus software and routinely released patches should be regularly updated to protect users against computer viruses and other malicious software. All measures should be taken to limit the amount of personal information that browsers can transmit without the users consent. Organizations should restrict employee's web browsing activities so that company's sensitive information is not compromised.

B. Server side Security

Server side security is very important and steps that protect the web server and the machine should be taken. The mechanism against denial-of-service attacks should be in place. The firewall systems and operating system should be properly configured to secure the servers.

C. Communication Channel Security

This deals with measure to protect private or sensitive information in transit from unauthorized third party. Any unauthorized party may intercept the sensitive or private information and tempered with or misuse the information. The main remedial action for such problems is use of cryptography algorithm to protect the information while in transit.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

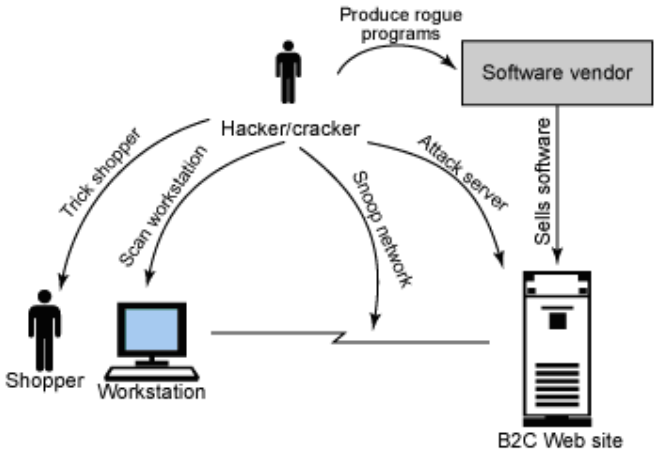

Figure 1. Points the attacker can target

D. Tricking the Shopper
The attacker tracks shopper's behavior gathers important information and uses that information against the shopper. The attacker normally lures shoppers with attractive offers on social websites [13].

E. Snooping the Shopper's Computer
There are various software tools available through which attacker can make entry into shopper's computer and scan ports to detect entry points into system. After gaining access to the shopper's machine, the attacker can scan his file system for any sensitive information such as user identity and password. Users normally do not configure the firewall to safeguard against security threats from snoopers.

f. Guessing Passwords
The users normally keep very weak passwords so that they could be remembered easily. This is susceptible to guess by attacker. The attacker may try to guess password manually or by any software if attacker knows something about the shopper. For example, if the shopper uses their pat's name or his own name as the password. The attacks by using software tools to guess the password etc are more likely to succeed than manual guess as number of tries increases significantly.

H. Server security and server exploits
In this category, attacker finds out the types of software used by analyzing the site and detects loopholes and lacunae in the site. He also tries to find out what security measures and software patches are being used. He then tries to exploit theses loopholes. Some expert attackers would find a weakness in software installed on the system; exploit the same to access the system. This is very effective attack. With so many servers online, there is a small probability that a system administrator forgot to apply a patch.

Server exploits refer to techniques that gain administrator access to the server. This exploits is the most dangers because the attacker can make limitless damage. With a server exploit, you access control of the merchants and all the shoppers' information on the site and can use that for your benefit. Buffer overflow attacks and executing scripts against a server are two major server attacks. In a buffer overflow attack, the hacker takes advantage of specific type of computer program bug that involves the allocation of storage during program execution. The technique involves tricking the server into execute code written by the attacker [13].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

IV.BASIC SECURITY THREATS

The rapid increase in use of e-commerce is accompanied by rise in the number and kind of attacks against the security of online transactions. The vulnerabilities that these attacks exploit range from loopholes in third-party components utilized by websites, such as shopping cart software to different types of vulnerabilities such as SQL injection, cross-site scripting, information disclosure, path disclosure, price manipulation, and buffer overflows.

A. The Distributed Denial of Service (DDoS)

Denial of Service (DoS) attacks make an attempt to prevent legitimate users from accessing some services or resources, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities [2]. Distributed denial of service attacks target one or more of the thirteen Domain Name System root name server clusters. The root name servers hold most critical component of the Internet infrastructure that translates domain names to Internet Protocol (IP) addresses. Every operation on Internet uses Doman Name System and Attacks against theses could impact operation of the entire Internet services, rather than just specific websites. However, the root name server infrastructure is made highly robust and reliable by deploying distributed and replication of databases.

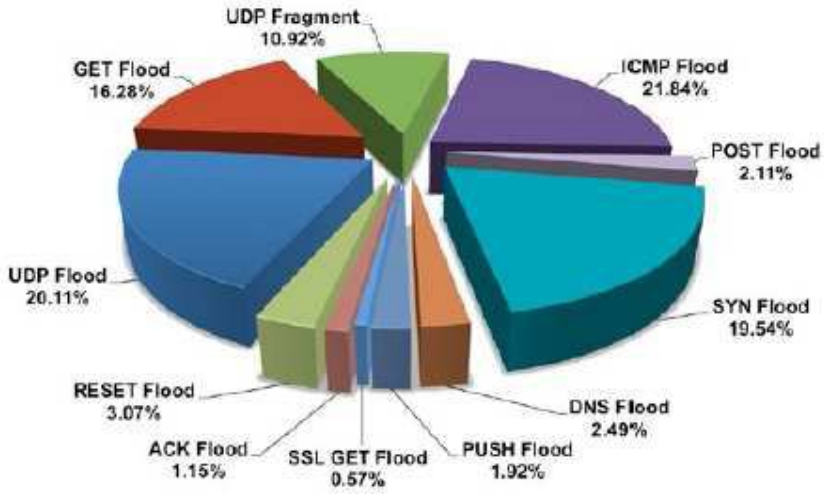

Figure 2 Total DDoS attack types in percentage

DoS attack affect the availability of site to users as server is overwhelmed with fake requests generated by attackers. DoS attack scripts are the most common, effective and easiest to implement attacks available on the WEB. No actual damage is done to the victim site. It would be every businessman's dream to be in this situation if the incoming packets were legitimate customer orders. The Distributed Denial of Service (DDOS) attacks are the latest evolution of DoS attacks and their success depends on the inability of intermediate sites to detect, contain and eradicate the penetration of their network. This attack creates problem not only to the target site, but also create congestion in the entire Internet as the number of packets is routed via many different paths to the target.

DDOS compromises the entire network and slave daemons are installed on the individual machines. These slave daemons can launch an ICMP, SYN, UDP or surfs flood attack but do so only at the command of master systems that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

were also compromised. The hacker sends the attack command to the masters, each of which relays the command to the slave daemons. It is quite possible to have tens of thousands of machines launching the attack against a single site.

The detection and removal of a DDOS attack by the compromised networks is very difficult from the master and slave programs. This failure could be caused by a number of reasons: lack of system administrator experience, lack of base security standards for each machine, lack of intrusion detection software to notify the admin or a management decision to not get involved. The most dangerous of these is the Windows 9x variant called win-trinoo because there are millions more Windows systems than servers.

The Ponemon Institute study estimates that the average cost of one minute of downtime due to a DDoS attack is $22,000. With an average downtime of 54 minutes per DDoS attack, this amounts to a heavy toll. Obviously, the costs depend on several variables, such as your business segment, the volume of online business, competitors, and your brand.

B. SQL Injection

SQL Injection is an attack method that exploits application vulnerability. Because the present encryption protection only can guarantee the security of data transmitting on the internet, but cannot check the content of data content filled by the user, and sent to the web server. If the attacker has filled the data that include the vicious SQL query instruction in the web page form, these query instruction together with HTML file will drill through the firewall and reach at to web server. When it is executed on the server**,** the vital information will be compromised. **[**3]. A successful SQL injection attack enables a malicious user to execute commands in our application's database by using the privileges granted to our application's login. Basically two major kinds of attacks are there. First-order attacks are when the attacker receives the desired result immediately, either by direct response from the application they are interacting with or some other response mechanism, such as email. Second-order attacks are when the attacker injects some data that will reside in the database, but the payload will not be immediately activated.

C. Price Manipulation

This is the most common attack. The total payable price of the purchased goods is stored in a hidden HTML field of a dynamically generated web page. In this attack an attacker can use a web application proxy such as Achilles to simply modify the amount that is payable, when this information flows from the user's browser to the web server. The final payable price can be manipulated by the attacker to a value of his choice.

D. Session Hijacking

Session hijacking refers to taking control of a user session after successfully obtaining or generating an authentication session ID. The attacker mostly uses brute force or reverse engineered session IDs to get control of legitimate user's web application session while that session is still in progress. HTTP is stateless, so application designers had to develop a way to track the state between multiple connections from the same user, instead of requesting the user to authenticate upon each click in a Web application. A session is a series of interactions between two communication end points that occurs during the span of a single connection. When a user logs into an application a session is created on the server in order to maintain the state for other requests originating from the same user. Applications use sessions to store parameters which are relevant to the user. High-jacking a session is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. This attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections.

E. Cross-site script (XSS)

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems they rely on. Exploiting one of these, they fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

information maintained by the browser on behalf of the user. Cross-site scripting attacks are therefore a special case of code injection

The expression "cross-site scripting" originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain (a *reflected* or *non-persistent* XSS vulnerability). The definition gradually expanded to encompass other modes of code injection, including persistent and non-JavaScript vectors (including ActiveX, Java, VBScript, Flash, or even HTML scripts), causing some confusion to newcomers to the field of information security.

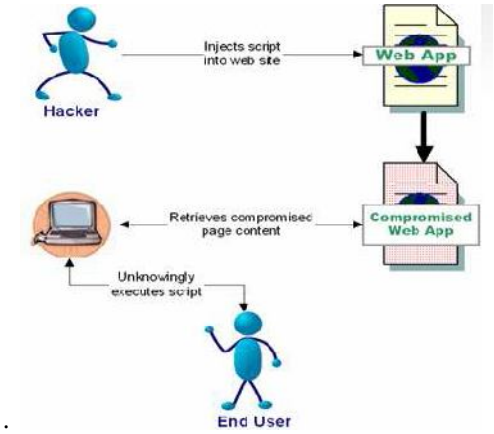

Figure 8 Cross-site scripting

V. OTHER SECURITY THREATS

Since inception of e-commerce, a lot of progress in the area of processing & storage of credit card information has been made. This progress has helped in creating customer trust in e-commerce transactions. Customer trust in e-commerce systems is very important for these systems to become successful and popular among masses. Unfortunately, the attackers also have the developed sophisticated methods to steal customer information and hence compromising web application security has become easier [15]. Additionally, attackers may also exploit viruses, worms, Trojan horse, bots, EXE file, browser parasites, adware, and spyware etc to compromise the security of the e-commerce systems.

VI. PROTECTING THREATS

The security of sensitive information such as credit card from attackers must get highest priority and every precaution must be taken to ensure security of online transactions through credit card. The Payment Card Industry (PCI) has laid down set data security standards and mandates compliance with it [15]. PCI regularly monitors and ensures that every successful attack against an ecommerce site that compromises credit card data is resolved. Despite attacks by hackers and crackers, e- Commerce remains a safe and secure activity for business [17].

A. Personal Firewalls

When connecting our computer to a network, it becomes vulnerable to attack. A personal firewall helps protect our computer by limiting the types of traffic initiated by and directed to our computer. The intruder can also scan the hard drive to detect any stored passwords. Many computers are infected by spyware of some sort. Most are 'harmless', but an increasing number pass into viruses that will steal and transmit confidential information, even memorizing the keystrokes of passwords.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

B. Secure Socket Layer (SSL)

Secure Socket Layer is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents. SSL allows transferring data in an encrypted form. All information that a customer might want to keep private should be transmitted via SSL. Such information should definitely include credit card number and related information, and may, depending on the type of business, include customer's name, address, and the list of products that the customer is buying. It should also include the customer's password and order ID [13].

The SSL certificate is issued to the server by a certificate authority authorized by the government. When a request is made from the shopper's browser to the site's server using https://, the shopper's browser checks if this site has a certificate it can recognize.

C. PCI Standard Compliance

In 2004 five different credit card security programs merged to form the Payment Card Industry Security Standards Council (PCI DSS) with the purpose of creating an extra level of protection for card issuers making sure that merchants (both online and brick and mortar) meet basic levels of security when storing, processing, and transmitting cardholder data. To set a minimum level of security, the Payment Card Industry set 12 requirements for compliance that fall into one of six groups called control objectives.

The control objectives consist of: build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, maintain an information security policy Companies that fail to comply with the PCI DSS standards risk losing the ability to process credit card payments and may be subjected to audits and fines. Credit card details can be safely sent with SSL, but once stored on the server they are vulnerable to outsiders hacking into the server and accompanying network. A PCI (peripheral component interconnect: hardware) card is often added for protection, therefore, or another approach altogether is adopted:

SET (Secure Electronic Transaction).

D. Digital Signatures and Certificates

Digital signatures meet the need for authentication and integrity. To vastly simplify matters, a plain text message is run through a hash function and so given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged (message has not been tampered with). Very often, the message is also time stamped by a third party agency, which provides non-repudiation. This is a digital document issued by the CA (certification authority: VeriSign, Thawte, etc.) that uniquely identifies the merchant. Digital certificates are sold for emails, e-merchants and web-servers [1].

E. Web Server Firewall

A web server or web application firewall, either a hardware appliance or software solution, is placed in between the client end point and the web application. Web application firewalls protect cardholder data because all web layer traffic is inspected looking for traffic that is meant to exploit known vulnerabilities as well as patterns that may suggest a zero-day exploit being launched against the application. A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines. A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts. Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is a resource placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall. These servers are closely monitored, and any access by an attacker is detected. Also, a Firewall can act as a “Proxy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Server". For example, if you have to use your e-Commerce Server to access other Web sites on the Internet, the Firewall will act as the intermediary between our e-Commerce Server and the Internet. The security advantage here is that our e-Commerce Server really never interfaces with the outside world [13]. All of the data packets that come from the Internet is first received by the Firewall, and are inspected. After inspection, they are then directed to our e-Commerce Server. Another security method you can use for a Firewall is called "Stateful Inspection". With this, only key parts of the data packet are examined, not the entire contents. For example, information in the data packets that are sent to the outside world from our e-Commerce server is compared to the information in the inbound data packets that are received by the Firewall which protects our e-Commerce Server. If there is a reasonable match in the information, the data packets are then allowed to enter the network which houses our e-Commerce Server. This is also known as "Dynamic Packet Filtering", vs. "Static Packet Filtering", which is the establishing of conditions mentioned previously. The security level to be established on the Firewall depends upon the level of security you want to implement to protect our e- Commerce Server.

F. Password policies

Ensure that password policies are enforced for shoppers and internal users. A sample password policy, defined as part of the Federal Information Processing Standard (FIPS) is shown in the table below.

TABLE I

FEDERAL INFORMATION PROCESSING STANDARD FOR PASSWORD POLICY

Policy	Value
Reuse user's previous password	No
Unsuccessful login delay	10 seconds
Matching user ID and password	No
Maximum occurrence of consecutive characters	3 Characters
Maximum lifetime of passwords	180 days
Minimum number of alphabetic characters and numeric	1 each
Minimum length of password	6 Characters

We may choose to have different policies for shoppers versus our internal users. For example, we may choose to lockout an administrator after 3 failed login attempts instead of 6. These password policies protect against attacks that attempt to guess the user's password. They ensure that passwords are sufficiently strong enough so that they cannot be easily guessed. The account lockout capability ensures that an automated scheme cannot make more than a few guesses before the account is locked.

G. Installing Recent Patches

Software bugs and vulnerabilities are discovered every day. Even though many of them are discovered by security experts, rather than hackers, they may still be exploited by hackers once they became a public knowledge. That's why it is important to install all software patches as soon as they become available.

H. Intrusion Detection and Audits of Security Logs

One of the cornerstones of an effective security strategy is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers. Suppose that you have implemented a password policy, such as the FIPS policy described in the section above. If a shopper makes 6 failed logon attempts, then his account is locked out. In this scenario, the company sends an email to the customer, informing them that his account is locked. This event should also be logged in the system, either by sending an email to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

the administrator, writing the event to a security log, or both. We should also log any attempted unauthorized access to the system [13].

VII. CONCLUSIONS

Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online. e- Commerce is growing rapidly and numbers of technologies have converged to facilitate the proliferation of e-Commerce. The best we can do is to show that a specific system is resistant against a set of well-known attacks. It is important to keep in mind that while each of these security measures described do afford a good sense of protection, we should not just use only one of them as our means of defense from threats and attacks. Much of the security today is addressed as an audit activity that mostly relies on the penetration testing such testing activities often attempt to identify vulnerabilities that belong to certain categories of threats and use tools that are tailored around these threats. They may have security policies that auditors follow which require them to check a specific list of the things, but they often fall short of identifying vulnerabilities that a result of the way the application logic has been custom developed. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

REFERENCES

[1] E-Commerce and Security, http://www.it.uu.se/edu/course/homepage/ehandel/vt08/
[2] A. Kahate, Cryptography and Network security, Tata McGraw Hill Education Private Limited, 2nd edition, 2008
[3] SQL Injection, http://en.wikipedia.org/wiki/SQL_injection
[4] Security Response, http://securityresponse.symantec.com/avcenter/refa.html
[5] C. V. Berghe, J. Riordan, and F. Piessens, *A Vulnerability Taxonomy Methodology applied to Web Services*, IBM Zurich Research Laboratory, 2005.
[6] R. Ganesan, M. Gobi, and K. Vivekanandan, \A novel digital envelope approach for a secure e- commerce channel," *InternationalJournal of Network Security*, 2010.
[7] 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.
[8] F. Nabi, \Secure business application logic for ecommerce systems," *Computers & Security*, pp. 208{217, 2005.
[9] Qi XIE, Lihong ZHAO. Research and realization of web services security. *Computer Engineering and Design*,2007,
[10] Zhu Lingxi. *E-Bunsiness Security. BeiJing.* Beijing Jiaotong University. 2006.
[11] W3C Working Group Note, "Web services architecture", http://www.w3c.org/TR/ws-arch, 2004.
[12] Apache Software Foundation, "Filters - Apache HTTP Server," http://httpd.apache.org/docs-2.1 /filter.html, Nov.2004.
[13] E-commerce http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney. html
[14] Ravi Kalakota, Andrew B. Whinston. Electronic Commerce: A Manager's Guide, Addison-Wesley, ISBN: 0-201-88067-9
[15] Critical Threats e-Commerce hosting, http://www.plaveb.com/blog/3-critical-threats-toecommerce- hosting
[16] Threats e-Commerce Server,http://www.technologyexecutivesclub.com/Arti cles/security/artThreatsto Ecommerce Servers.php
[17] E-Commerce site security, http://www.applicure.com/solutions/eco
[18] e-commerce-security