"Securing E-commerce Application against Various Vulnerability"

Pranay chauhan, Rahul pawar
M.E., Information Technology
pranaychauhan1985@gmail.com,

Abstract

Internet play an important role in our daily life the use of internet is increasing rapidly and as the role of ecommerce application is also increases some of these application are quite secure and some of them are unsecure many vulnerability can easily exploit them .Security measure are not effective.[1]. And in order to protect these ecommerce application many measures have been taken such as client side can be secure by antivirus, firewall and using secure web browser in which SSL or TLS is inbuilt which will provide secure communication between the web browser and web server but then also intruder can easily target these application and make use of these application. Our paper would mainly focus on these vulnerability, Types of vulnerability and how these vulnerability mainly can be tested by various testing approach and how to secure different e commerce application against the different vulnerability and what are the different measures should b taken in order to protect the system against these vulnerability and how data integrity, non repudiation, confidentiality can be maintain

Keywords*:* - Vulnerability, testing, SSL, PKI

1. Introduction

As we know that when buying or selling is done over the internet many preventive measures should b taken in order to protect against various threat. Many software based solutions have been developed in order to protect against these threat but then also many threat can easily target these application [1].various vulnerability such as bad operating system configuration, proper maintained of software, password and access control, malicious software such as malware services these vulnerabilities can easily exploit the services. The most common of these systems management process failures exist in the following areas: System software configuration Applications, software configuration, Software maintenance, User management and administration figure -1. Shows the various vulnerability found in the many hosts passwords and access control is the most popular form of vulnerability because when user type the passwords in the system then this password gets verify by the server so in between the web browser and the web server the attacker can easily apply the various active and passive attacks by which the passwords can be easily occupied so maintaining the SSL between the server and client side this vulnerabilities can be avoided in case of maintaining the better software maintained and avoiding the various unauthorized WebPages by using the better antivirus software and proper management can be done

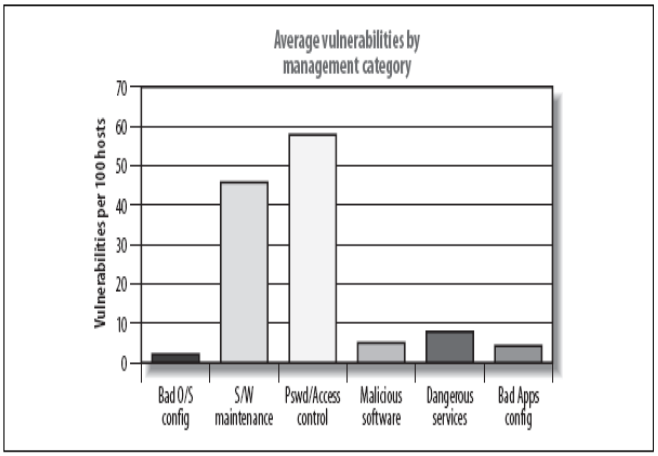


Figure F-1. Average vulnerabilities by management category

These vulnerabilites can be easily identified by the assessment proper security assessment can easily identify these vulnerabilties and the various testing which are involved in during to identify these vulnerabilities such as [6].

- *Web application testing* involves post-authentication assessment of web application components, identifying command injection, poor permissions, and other weaknesses within a given web application. Testing at this level involves extensive manual

qualification and consultant involvement, and it cannot be easily automated.[6]

- Full-blown *penetration testing* - involves multiple attack vectors to compromise the target environment.
- *Onsite auditing* provides the clearest picture of network security. Consultants have local system access and run tools on each system capable of identifying anything untoward, including root kits, weak user passwords, poor permissions, and other issues. [6].

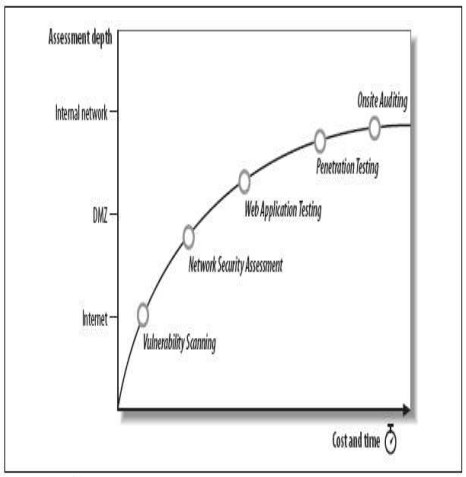
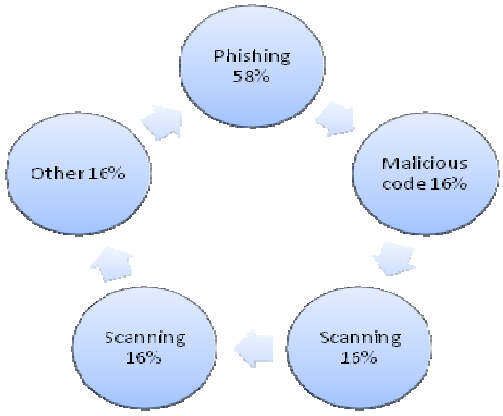


Figure 1-1. Different security testing services

The above figure 1-1 describes about the various security testing services [2]. In this vulnerability scanning, network security assessment, web application testing, onsite auditing etc these testing can be done against the various networks. By these various testing various open ports can be identified. Various techniques [6]. For network scanning such as Nmap, Nessus etc which mainly perform the fingerprinting stealth scanning and traffic can be scan low load traffic can be scan by the Nmap, while high load traffic can be scanned by the Nessus scanning tool then the assessment and at last the exploitation can be done in which mainly Metasploit framework is used to perform the exploitation i.e. how to make use of these vulnerability. So various approached should be maintain properly in order to provide the better security services the Above paper would focusing on the vulnerability and then protection against these

2. Problem Domain

The main problem with e commerce application is that as the role of Online transaction is increasing and the role of attackers, intruders is also increasing they were many cases in India were the [3].most of them of phishing attacks, then malicious attacks, and there is and drastic growth in the scanning attacks as mention earlier many tools were there by which scanning is done these tools are Nmap, Nessus, active scanner, Eeyes retina,etc and other tools were of web based testing such as active scanner and passive proxy are web based tools



v

Figure.2-1 Security Incident report [3].

There is a cyber Intrusion during January fig. (2) [2].according to this report phishing, virus attack, and spam mail are the most prior sources of attack

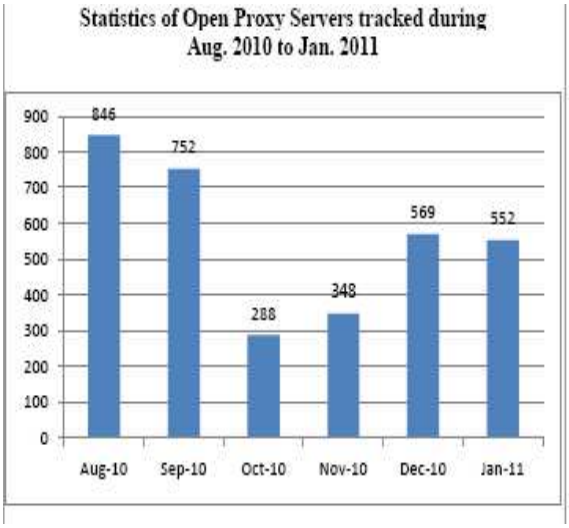


Figure.2-2 Security Incident report

As per CSI/ FBI Cyber crime survey report vulnerability in our system is responsible for average loss of $ 215,753. [3] If we talk about India. India ranks 14th in phishing attacks [3]. In India they are many cases are thereof email fraud these cases are mainly of phishing attack, spoofing attack, virus attack.

According to report in India the mostly attacks were from Nigeria. So in order to protect against such type of attack the security at email is needed and as the various security protocol are not good enough secure to provide security so the high security is needed.

3. Solution Domain

In order to provide better security the better measures should be taken here the vulnerabilities can be differ from operating system to operating system different O.S. has different vulnerabilities various tools can be used in order to provide better scanning and better security such as enumeration can be perform by the Nmap, Nessus which mainly scan the network traffic both the tools can be used as a network scanning and they also perform the stealth scanning and fingerprinting ,Nmap mainly perform the scanning at low load network traffic while Nessus mainly scan the low load traffic and other tools which are mainly available for scanning are eyes retina and qualis guard the main role of scanning is to find the domain, and IP Address and port number by which the vulnerability can be exploit other tools for web based scanning is the active scanner and passive proxy by this active scanner and passive proxy tools the web based testing can be easily be performed. The reconnaissance can be easily done by the tools such as Who is, Dig, Nslookup, Tracert these tools mainly perform the reconnaissance other approach by which the these vulnerability can be avoid is by using the proper configuration of operating system, updating the software regularly and mainly managing the secure database[4].. The malicious software vulnerability can be avoided by using the proper antivirus i.e. registered antivirus and using the safe and secure browser connection this will avoid many of the problem which mainly cause by unsecure connection the browser should maintain the SSL or TLS by maintain the secure socket layer the web browser and web server can be communicate properly and connection will be secure the secure socket layer mainly make the use of handshaking protocol by which server authentication and client authentication can be done in this secure socket layer another protocol is the alert protocol which mainly alerts the peer entities about the error such as fatal error and non fatal error and the third protocol is record protocol in which an data can be fragmented then compressed and addition of MAC is done and then encryption and at last the append header is performed which will make the proper security the secure socket was get modified and after words it was named as a transport layer security which mainly work over the transport layer so the web browser and web server can have a secure connection and various malicious activity can be avoided.[4]. By implementing the firewall the unauthorized packet can also get filtered as the firewall does not allow the unauthorized packet to enter your network it can be implemented in software part as well as hardware part other various and other measures for maintaining the online security by which the authentication can be maintained is to maintain the Kerberos version 5 which will also maintain the authentication the digital certificate can also be maintain to provide the authentication , the digital certificate is to issued by the certifying authority which is an trusted agency so privacy and the authentication can be maintained in proper manner. The role of biometric can also be important in the places where the more authentication is needed the different biometric mechanism can be used as per need in case of online payment with the client side wallet the physical biometric can be important this will avoid many cases of online fraud .and as the role of e commerce application is increasing rapidly the role of attackers also great increases so proper security measures has been taken in order to provide security.

4. Expected Outcome

The main use of these tools and techniques is to enhanced securing measure which would make secure environment the advantage of using the security approaches is to maintain proper data integrity, confidentially, authentication which will make e commerce application secure and less vulnerable these vulnerability can be over come by the above approaches the various application which can be secure and they can be used in

- Banking system
- Defense system
- Company portal
- Mailing server, payment server
- secure Finance system

5. Conclusion

The above paper defined the different types of vulnerability and how these mainly affect the e commerce application in different aspect .The various tools that can be used in order to perform the testing various testing that can be done at the client based and server based and how the exploitation of data can be done and the several approach that can be used in order to provide better security, how the security can be maintain properly and the basic goals of security can be achieved

6. References

[1] William Stalling, *"Cryptography & Network Security Principles and practice" 3rd* edition, PearsonEducation 2005.

[2] *"Report on Cyber security: CERT VULNERABILITY NOTES"* CERT Gov. of India http://www.cert-in.org.in/ *(*Accessed 18 March.)

[3]Cases of the phishing attack in India [Online].Available http://www.thesecurityblog.com/2011/04/phishing-attacks-on-indian-banks-on-the-rise/ *(*Access16 March.)

[4] White papers on Guide to securing intranet and extranet servers from [Online] available at*:* http://www.windowssecurity.com (acessed: 14 Feb.)

[5] Malware spreading countries [Online] available at*:*http://www.spamfighter.com/News-13363-Kaspersky-Lab-%E2%80%93-China-Hosts-Highest-Malware-Laden-Websites.htm (accessed 29 March)

[6]. Chris McCabe, "network security assessment" Principles and practice" 3rd edition, Publisher: O'Reilly Media March 2004.