Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

Database Security for E-Commerce Websites

Karan Gadgil
Department of Computer Engineering
RMD Sinhgad School of Engineering
Pune, India

Samiksha Potey
Department of Computer Engineering
RMD Sinhgad School of Engineering
Pune, India

Karan Pardeshi
Department of Computer Engineering
RMD Sinhgad School of Engineering
Pune, India

Karan Gupta
Department of Computer
Engineering RMD
Sinhgad School Of
Engineering Pune, India

Abstract **- With the high speed internet trend embracing the field of computer the E-commerce field is growing day by day due to its services provided to the customers. E-commerce includes management of the database, ordering, delivery, etc. in easy steps which is handy due to growing world. More and more companies are intimated by this technique so as to provide efficient services to their respective customers. However, this technology comes with lot of challenges like being attacked by hacker, intrusion of third party, etc. This causes the service provider as well as the user using the service at huge loss. This can also cause leakage of important information. This causes decrease in quality of security and trust of the user. Therefore, in order to keep up with the growth of e-commerce e-commerce should gain trust of their users as well as prevent their services from being attacked by the intruder. In this paper different types of security issues faced by the e-commerce will be discussed in general and also the literature survey on the existing technologies and also the measures to deal with the security issues will be well elaborated.**

Keywords - Database security, E-commerce website, Hacker, security issues

INTRODUCTION

In recent years due to the increasing growth of computer and internet, it's application have affected the society in several fields such as military, civil services, educations, health services, transport services, e-commerce, etc. With this there is an increasing trend of e-commerce website as they provide services which are easy and convenient to use. The customers day by day are also giving remarkable response to e-commerce. To illustrate, some of the important e-commerce websites are flipkart, amazon, OLX, myntra, etc.Through e-commerce website there is variety of activities taking place such as online transaction, inventory management, database having the details of the customers/users or also the details of the product, etc. However with the growing trend of the e-commerce website there is also a considerably growing problem that the e-commerce website can be hacked by the hackers and the information can be used by the hacker, for example the hacker if able to hack the system can use the details of the payments made by the customers or also can make the changes in the database consisting the information about product. Also if the hacker gains the information about customer's details they can even hack into the customer's system allowing the hacker to encrypt the user's data and then demand for money or ransom to unlock or decrypt the data, also they can use the customers details for gaining information about their bank details or credit cards.

Many such attacks have been detected in recent years that made use of customer's information to block or hack their system such as petya, ransom ware, etc. This has caused heavy loss for the customer as well as the administrator. For example using ransom ware attack (in which hacker holds a computer hostage and encrypts the data on the system, in order to decrypt the data the victim has to pay the ransom,) more than two lakhs system were hacked in almost 150 countries which caused leakage of important data and information which also resulted in heavy loss.

In order for e-commerce websites to progress and to continue, there has been lot of work which has being done to prevent the hackers from hacking the system and to protect the user's details. However till date there has been no perfect solution for such attacks or hacking of the system. In this context, it would be interesting to know the research and development works which have been carried out with these attacks and how they can be prevented and if attacked how can we overcome the attack.

One of the measures that can be taken to prevent such attacks is to have pre-installed software in the computer protecting it from various attack and stop data from being hampered. However many of the users do not install these kind of software as they are not well aware of these software's. Mostly the users that use computers having Windows Operating System have been attacked according to the recent study. So to prevent the attack we can also opt for different operating system. However these ways are also not full proof and are not used commonly. Also the E-commerce service provider has to update the all the security measures and also prevent the attack from taking place.

Some of the existing work and methodologies have been developed to overcome these attacks. Following is a measure that can be taken if attacked by the attacker, victim needs to be calm and composed and not panic, and the connection of the internet should be removed as soon as possible. This may help in tackling with the attack. Also

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

there is a system which provides security to the server and if attacked by the attacker helps to analyze the information of the attacker and also trace its location. However these methods also do not guarantee the 100 percent protection from the website being hacked or attacked as it needs skilled techniques which have to be learning.

Since the time E-commerce was introduced in the world, research was started for the security issues that were faced by it. As there is no appropriate solution to these issues, different E-commerce service providers use different methods or take different measures so as to provide security to their service as well as the customers .The aim of the study to study the techniques and systems which have been used to prevent hacking in e-commerce and review applicability of such techniques and systems also to study the developments in anti hacking systems.

The material that is used to conclude this study is surveyed from the IEEE papers and some of the similar journal. The rest of the paper is organized as follows: Section 2 presents a summary on E-commerce architecture. Section 3 categorizes and classifies different types of security issues regarding the database security of the E-commerce website. Section4. Finally the last chapter concludes the methodologies that have been studied.

E-COMMERCE

E commerce (Electronic commerce) is a business model for small to large business organizations to carry out transactions faster using the electronic medium. The four major types of E commerce based on the parties involved in the business are business to business, business to consumer, consumer to consumer and consumer to business. The rise of E commerce can be attributed to the highly significant advantages that it offers to entities on both side of business. It causes reduction in buyer's sorting out timeless time is spent in resolving invoice and order discrepancies, increased opportunities for buying alternative products and allows businesses to be carried out from any place in the world.

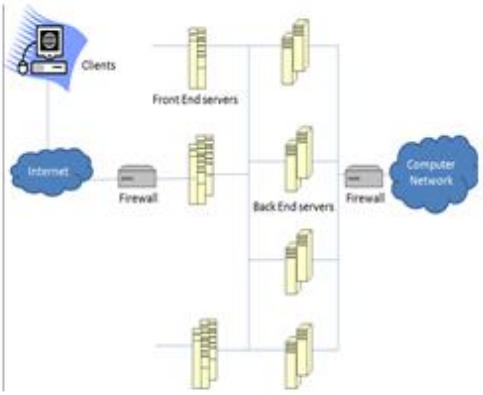

Fig. 1: A simple architecture model for E-Commerce

Along with all its advantage, E Commerce remains susceptible to various threats. Studies have shown that prominent attacks on online commerce are increasing at an alarming level. A study conducted by Ponemon Institute and commissioned by NetWitness shows that online threats are on the rise. The research investigated 591 IT and IT security practitioners and showed that 83 percent of them believe their companies has experienced some attacks, with 71 percent reporting a growth of threats over the past 12 months. These attacks aim mainly at stealing sensitive data including source code, non-financial business information, confidential information, and financial information [1].

E-Commerce Threat Categorization:

1) Intellectual Property Threats: Illegitimate use of content by a browser from a website without the owner's consent.

2) Client computer threats: Sometimes client computers may impose for electronic threats like Trojan horse, viruses. Which enters the client computer without user's knowledge, steal the data and destroy or crash the client computer.

3) Communication channel threats: As internet allows anyone to send and receive information through many networks. Data may be stolen, modified by unauthorized users of hackers. Hackers can develop software to steal the user identification and pass words as well.

4) Server threats: Denial of service is a major threat for the servers, where hackers generate a program which sends many requests from the client side that cannot be handled by the server. Spamming is another important threat for the servers. To protect our server from the above threats we can use authentication for web access, digital signatures and firewalls.

Various threats which affect the E Commerce substantially are discussed:

SQL injection attack consists of insertion (or "injection") of unauthorized SQL database statements into a vulnerable SQL data channel. This is classified under communication channel threats. Typically, targeted data channels include stored procedures and Web application input parameters. These injected statements are then passed to the database where they are performed. Using SQL injection, attackers may gain unlimited access to a whole database and to the potentially sensitive information these databases contain. Sources for SQL Injection can be:

1) Injection through user input; malicious strings in web forms.

2) Injection through cookies; modified cookie fields contain attack strings.

3) Injection through server variables; headers are manipulated to contain attack strings.

4) Second-order injection; Trojan horse input seems file until used in a certain situation. Attack does not occur when it first reaches the database, but when used later on. [2]

Price Manipulation is a vulnerability that is almost completely unique to online shopping carts and payment gateways. In the most common occurrence of this vulnerability, the total payable price of the purchased goods is stored in a hidden HTML fields of a dynamically generated web page. 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. This information is eventually sent to the payment gateway with whom the online merchant has partnered. If the volume of transactions is very high, the price manipulation may go completely unnoticed, or may be discovered too late. Repeated attacks of this nature could potentially cripple the viability of the online merchant [3].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

Cross-Site Scripting (XSS) is a technique where the option of user's input to a website is rendered vulnerable as it can be exploited to inject a malicious code script which then consequently gets loaded into every other user's web browser that visits the website. XSS working: 1) the attacker injects a payload in the website's database by submitting a vulnerable form with some malicious JavaScript. 2) The victim requests the web page from the website. 3) The website serves the victim's browser the page with the attacker's payload as part of the HTML body. 4) The victim's browser will execute the malicious script inside the HTML body. In this case it would send the victim's cookie to the attacker's server. The attacker now simply needs to extract the victim's cookie when the HTTP request arrives to the server, after which the attacker can use the victim's stolen cookie for impersonation.

Ransom ware is a kind of malware which is deployed by the hackers to lock or kidnap file from victim's computer system. It includes data like documents, databases, source codes, pictures, videos, etc. The ransom amount demanded is in Bit coins. Several of its subtypes and the aspects related to them are presented in the following table.

Ransom ware	Canonical Dates	Crack able or not	More details
Apocalypse	June 2016	Crack able	Weak algorithm
Cerebra	March 2016	Was crack able, currently not	The second-level key used to be leaked by its C & amp; C server.
Crypto Wall	2014	Non crack able	It cannot run because C and amp; C server is down.
CTB Locker	2014	Non crack able	None
Jigsaw	April 2016	Crack able	Decryption key can be found in the ransom ware sample.
Locky	Feb 2016	Non crack able	It cannot run because C and amp; C server is down.
Petya	March 2016	Crack able	The second-level key can be found, because the cryptographic strength is weak
TeslaCrypt	Feb 2015	Crack able	The ransom ware author releases the first-level key (master key)
Torrent Locker	2014	Non crack able	None
Unlock92	June 2016	Non crack able	None

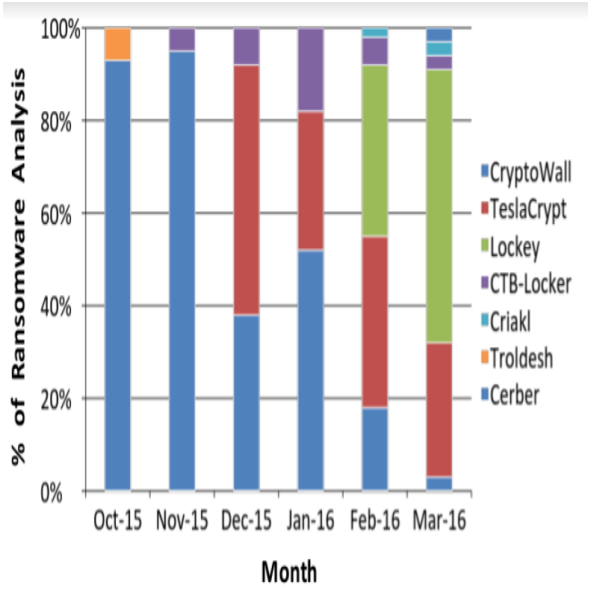

Fig. 2: Comparison between the ransomed attacks

Literature System:

In 2012, Puspendra Kumar [1] performed a survey on SQL Injection attacks, Detection and Prevention Techniques and described how attacks are implemented on the database using SQL Queries .The attacks were categorized on the basis of SQL Manipulation, Code Injection, Function Call Injection, and Buffer Overdo. Conclusively, a comparative analysis of different types of detection and prevention techniques of SQL Injection attacks was presented.

In 2011, Abdul Menem S. Brahma, Rabah N. Farhan, Hussam J. Mohammad [2] has proposed a protocol design for securing e-commerce transaction by using hybrid encryption technique. This method has increased the performance of cryptographic algorithms. This method ensured the confidentiality, integrity and the authentication in which AES Algorithm provided confidentiality, MD5 hash function provided integrity and modification of Diffie-Hellman ensured the authentication. The algorithm was tested for various sizes of messages. The experimental results demonstrated that model enhanced the interacting performance and also provided high quality of security service for e-commerce transactions.

In 2014, Mukesh Kumar Gupta, M.e. Govil, Girdhari Singh[3] have proposed a classification of software security approaches used to develop secure software in various phase of software development life cycle. It epitomizes static analysis approaches that detect weakness in coding phase of software development life cycle. More research will be needed to improve analysis technique for providing precise detection results.

Dr. M. A. Pund, Gajanan P. Bherde [4] analyzed various types of attacks found in web applications. These attacks were broadly categorized into seven types which include Cross-Site Scripting, Cross-Site Request Forgery, Structured Query Language Injection; Server is configuration and Predictable Page, Breaking Authentication

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

Schemes, Logic Attacks and Web of Distrust. In their paper various attacks were studied to detect and prevent such attacks and provide more security. It is clear that hybrid based detection system performed better than any other systems.

In 2012, Hatoon Matbouli, Qigang Gao [5] conducted a survey and analyzed e-commerce related security issues, the impact to E-commerce success, and the available integrated security strategies. They attempt to guide how to properly deal with the security threats that inimically affect e-commerce.

In 2016, Rhythima Shinde , Pieter Van der Veeken, Stijn Van Schooten, Jan van den Berg[6] comply a literature study and conducted interviews of the people victimized by ransom ware and a survey with random set of victimized and non-victimized by ransom ware – conclusions about the dependence of ransom ware on demographics like age and education are shown. Increasing threats due to ease of transfer of ransom ware through internet are also discussed. Lastly, they have affirmed the standing notion about ransom ware, that nearly all victims are unwilling or unable to pay the ransom.

EXISTING SYSTEM:

Intrusion Detection System:

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configuration and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

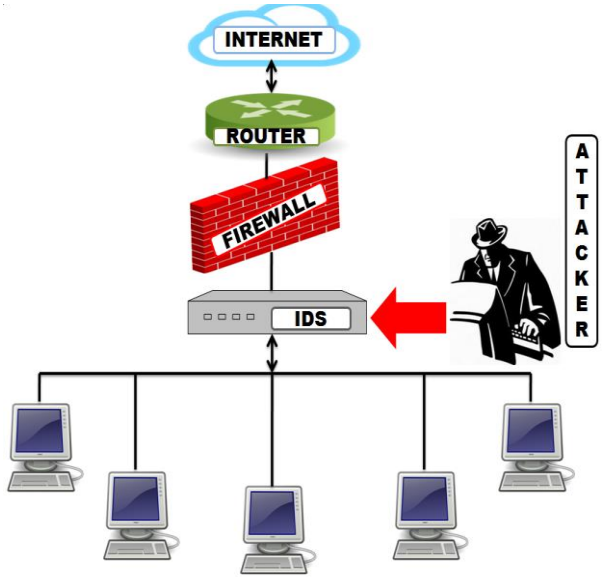

Fig. 3: IDS

CONCLUSION:

This paper presents the survey of different database security related issues like XSS, URL injection, and some prevention techniques. This paper also takes into account, various ransom ware attacks, their consequences and preventive measures. From literature survey, it is clear that Analyzer and Rollback system for data security against Ransom ware performs better than other systems. In future, more research will be needed to prevent the attacks and secure database.

REFERENCES

[1] Puspendra Kumar" A Survey on SQL Injection Attacks, Detection and Prevention Techniques" IEEE- 20180.

[2] Abdul Menem S. Rahma1 , Rabah N. Farhan2 , Hussam J. Mohammad3 "HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION" International Journal of Advances in Engineering & amp; Technology, Nov 2011. C
IJAET.

[3] Mukesh Kumar Gupta, M.e. Govil, Girdhari Singh" Static Analysis Approaches to Detect SQL Injection and Cross Site Scripting Vulnerabilities in Web Applications: A Survey" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India.

[4] Gajanan P. Bherde, Dr. M. A. Pund "Recent Attack Prevention Techniques in Web Service Applications" 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (IIIT), Pune.

[5] Hatoon Matbouli, Qigang Gao "An Overview on Web Security Threats and Impact to E-Commerce Success" 2012 International Conference on Information Technology and e-Services, IEEE.

[6] Rhythima Shinde, Pieter Van der Veeken, Stijn Van Schooten, Jan van den Berg "Ransom ware: Studying Transfer and Mitigation" 2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016, 9781-5090- 1338-8 c2016 IEEE.

[7] Krzysztof Cabaj and Wojciech Mazurczyk"Using Software-Defined Networking for Ransom ware Mitigation: The Case of Crypto Wall" International Journal of Advances in Engineering & amp; Technology, Nov 2014. CIEEE

[8] N. Angel, Dr. A. ChandraSekar "Distributed Denial of Service Attacks in Network Propagation Model with Web Service" 8th august 2016 c IEEE

[9] Igor Kotenko, Alexey Alexeev and Evgeny Mankov "Formal Framework for Modeling and Simulation of DDoS Attacks Based on Teamwork of Hackers-Agents"