Bachelor's Thesis (TUAS)

Bachelor in Engineering

Information Technology

2010

Said Sabir

E-COMMERCE SOLUTION

– CREATING A SHOPPING CART USING OPEN SOURCES (APACHE/MYSQL/PHP)

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology

Spring 2010 | 58

Instructor: Balsam al-Murrani

Sabir Said

Abstract

In recent years, the power of the Internet has popularized the notion of electronic commerce, which offers many advantages for businesses as well as regular daily life. It has made communication, collaboration, traveling extremely easy. Consumers can access the digital business environments with a click of a mouse and participate in on-line business transactions more easily than by the use of traditional methods. This evolution is a prime phenomenon in the modern business world.

This thesis work illustrates the basic concepts of E-Commerce as well as highlights the general operating mechanisms of a Shopping Cart. Through a collective study of Information and Communication Technology and Commercial activities running with its aid, this work is an attempt to understand the ideas and trends as well as the security matters of an E-Business. The Shopping Cart is used primarily in online retail stores that offer their products via the internet. It is a simple illustration of the offered products through a dynamic interface which is backed by various web technologies such as PHP Scripting / Web Programming Language Technology, MySQL Database and various other micro-web applications. This thesis was conducted by literature, articles released on the Internet, and discussions with experts.

Furthermore, this thesis has provided the basic concepts for developing an E-commerce site using a shopping cart with Internet technologies such as PHP, MySQL. The goal of this thesis is to provide a secure shopping cart for E-commerce that helps customers and merchants to confidently buy safely in the most popular sites on the web.

KEYWORDS: E-commerce, shopping cart,Open Sources, APACHE, MYSQL ,PHP

Foreword

My study was carried out in the Department of Information Technology at Turku University of Applied Sciences, during the years 2005-2010.

This thesis is based on building a secure shopping cart for E-commerce that helps customers and merchants to confidently buy safely in the most popular sites on the web. The work presented in this thesis could not be possible without the guidance and support of many people.

I am heartily thankful to my supervisor, Balsam Almurani, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of my thesis subject.

My gratitude goes to Poppy Skarli for her advice and help through my studies.

I am indebted to my mother, Jraynija Kaltoum, for her care and love. As a typical son in a Moroccan family, I am grateful to my father Ahmed Sabir who worked industriously to support his family and spared no effort to provide the best possible environment for me to grow up and attend school. He had never complained in spite of all the hardships in his life. Although they are no longer with us, they are forever remembered. I am sure they share my joy and happiness.

My dearest thanks go to my family, my wife, Amina Sabir, and our children, Hamza and Emilia, for their understanding, and incredible patience. Special thanks go to my wife for caring for our son Hamza during these years of my study. I would like also to thank my wife's family (Lähteenmäki), as well as expressing my apology that I do not mention them personally one by one.

Last but not least, thanks be to God for my life through all tests in the past five years. You have made my life more bountiful. May your name be exalted, honored, and glorified.

04.06.2010

Turku

TABLE OF CONTENTS

FIGURES

TABLE

1 INTRODUCTION

E-Commerce can simply be defined as the purchasing, selling, and exchanging of goods and services over computer networks (Internet, VPN or other private networks) where transactions or terms of sale or service are performed electronically through those networks. E-commerce has evolved as an integral part of the world economy, and is not limited to the Web. Most of the business activities nowadays include some form of e-commerce activities partially or completely [2].

Rapid growth in the Internet as well as other networking technologies, applications, ease of availability of information, advancement in overall Information and Communication Technology assisted in evolution of e-commerce as mandatory and universal operation in the world economy. Digitalization of information, and services increased the demand to access information fast and securely. This brought forth too many challenges but as the era of Information and Communication Technology is evolving in its rapid pace, new solutions are emerging. Traditional commercial activities are gradually being digitalized and business activities of new nature are evolving. Some of these businesses fully rely on the availability of information, its flow and foundation.

There are various business activities being performed on-line every second but the very basic yet powerful and mandatory one is the Shopping Cart. Still the major portions of the transactions carried out electronically are the transactions that include buying and selling products from a B2C model of E-Commerce. The mandatory resource for these types of transaction is the shopping cart.

A Shopping cart is usually a web application that contains information about the products offered for sale. Such information is usually the picture, dimension, price details of the product. As users go through the shopping cart, they can browse and view many products in different categories and buy the products if they want. So, this system usually includes a method for payment processing as well. Popular payment

processing methods that are commonly in use include some integrated web applications which connect through bank networks and third party payment processing tools such as Pay Pal

A Shopping Cart can simply be developed using Open Source technologies such as PHP and MYSQL. MySQL is a database server which is used to store the data dynamically in the web server and the PHP Scripting language is used to process all information. Every event can be recorded in the database using the PHP Scripting language. On the server side and in the infrastructure, there may arise some security issues which can be solved by using different tools and technologies.

2 E-COMMERCE MODELS AND CONCEPTS

2.1 Overview

E-commerce (electronic commerce) can be defined as the summation of all commercial activities being performed in, via or by facilitation of virtual space, i.e. Internet or the World Wide Web. All commercial activities running inside the electronic-business sphere can be regarded as E-commerce. E-Business commonly represents all types of commercial activities which are based on the Internet such as retail shopping centers, banking, stocks and bonds trading, auctions, real estate transactions, plane ticket booking, movie rentals and anything that could be operated in real world. Not only are some commercial transactions done directly in the electronic sphere, but personal services or other real world business are also represented online on the Internet. This way, the E-Business is growing as an independent, sophisticated and enormous operational section of the world economy.

E-commerce technologies provide a lot of opportunities to the real world business owners as well as every individual who wants to be a successful entrepreneur because unlimited information and tools and technologies are available in the World Wide Web.

These technologies are nowadays used for many types of transactions including those which are not based on the Internet. Credit card transactions, information verifications, business communications, marketing activities, research activities etc., are all based on these technologies. In this way, the e-commerce is growing as a separate arena of commercial spectrum as well as an integral part of the real world business transactions. There are plenty of advantages of running a business online, as well as several risks and challenges, too.

Security threats and fraudulence are growing in parallel to the growth of e-commerce concepts and technologies. All commercial activities are networked hence linked together by the World Wide Web; this simply means that there is a huge range of information traffic which, if not secured properly, could be leaked, stolen, destroyed, corrupted or misused. So, security is the prime consideration in e-commerce.

2.2 Types of e-commerce

Every commercial activity being performed on-line or through some kind of electronic instrument or instrument chain or through networked devices is independently a unique type of e-commerce activity. However, we can categorize all those commercial activities based on the involving parties into following types:

- Business to Business (B2B)

  If a company is engaged in some kind of commercial activities electronically or satisfying the terms for e-commerce activities with another company then this type of e-commerce is regarded as Business to Business (B2B) as illustrated in Figure 2.1.

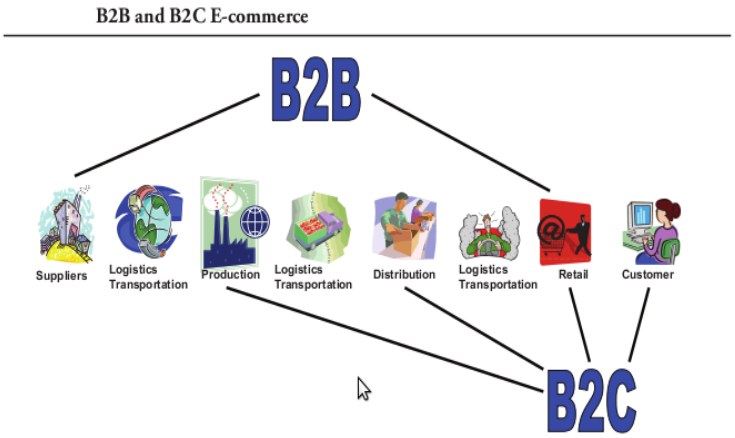


Figure 2.1 B2B and B2C E-commerce [1]

- Business to Customers (B2C)

  If a company is engaged in some kind of commercial activities electronically or satisfying the terms for e-commerce activities with its customer, then this type of e-commerce is regarded as Business to Consumer (B2C).

- Customers to Business (C2B)

  If a consumer is engaged in some kind of commercial activities electronically or satisfying the terms for e-commerce activities with one or more companies, then this type of e-commerce is regarded as Consumer to Business (C2B).

- Customer to Customer (C2C)

  If people are selling or buying products, services or information through a common platform, then they are engaged in Consumer to Consumer (C2C) E-commerce.

Among the above examples, B2B and B2C are abundant in number and popularity.

2.3 Benefits of e-commerce

Electronic commerce offers the companies many advantages.

- More effective marketing, more profits:

The adoption of on-line marketing by companies allows them to showcase their products and services in various parts of the world without interruption - throughout the day, seven days a week - giving these companies a greater opportunity to reap the profits, as well as access to more customers.

- Reduced expenses:

The process of preparation and maintenance of e-commerce sites on the Web is more economical than building retail markets or maintaining offices. Companies do not need to spend a huge budget on promotional activities, or to install expensive equipment used in customer service.

- Effective communication with partners and customers:

The scope of e-commerce is not limited to any distance or a border but it is limitless. This provides an effective way to exchange information with partners, and a good chance for companies to take advantage of the goods and services provided by other companies (i.e., suppliers).

- Benefits for consumers:

Several benefits for consumers such as saving of time and effort to find the right product, freedom of choice, price reduction etc. are easily achieved.

An e-business is not just another venture for business for companies but a whole new system of business in the world economy. Currently, it occupies a significant portion of world market and generates enormous revenue. Starting an e-business or adopting an e-commerce for running a business is not just profit-making but keeping up with the technological advancements, understanding the market development and going with the flow.

Electronic business, commonly referred to as "e-Business" or "e-business", may be defined as the application of information and communication technologies (ICT) in support of all the activities of business. Commerce constitutes the exchange of

products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses [7].

3 OPEN SOURCE

3.1 Overview

Open Source is a policy used in the management process of software systems development and it provides the Source Code as the programmer has written it. One of the most important features of Open Source software is its flexibility; the public users can modify it and develop it. The origin of the term Open Source can be traced in the end of the nineties ‘, when Eric Raymond attempted to find an alternative term for the term free software, which was misinterpreted as a free-ware. Generally we can define Open Source software in six points [5]:

- The freedom to redistribute the program.
- Availability of the source code, and the freedom to distribute it.
- Freedom to derive or modify the original program and freedom of distributing it under the same license of the original software.
- The absence of any discrimination in the licensing of any group or people.
- No identification of areas in which the program can be used.
- The rights in the license must be given for each program that is distributed.

3.2 Usefulness and importance

Open Source is nowadays one of the most important elements in software development; This was noticed a the few years ago with the emergence of high-level software in the various disciplines as Multimedia, Operating System, Web browsers, anti-viruses, Apache, MySQL, PHP, protection programs, and even games. What gives this type of software such importance is that anyone can add, modify, and develop it and then publish all that information on the Internet, and then give and receive comment by others and inform them of any problems or gaps. In addition other programmers can take this program and further develop it.

3.3 Examples of Open Source software

The Apache HTTP Server is free, Open Source and scalable. [6] According to the Apache, 'Net craft 'statistics over half of web sites use Apache as web server for their own sites. There exist many copies of it that are commensurate with the different operating systems, such as Windows and Mac and OS X and UNIX.
The Apache server is a flexible program and the strength and security of the medium and work environment work more efficiently under the UNIX platform, and is not good at all for large companies.

The MySQL database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching, and replicating the data it holds.

There are other kinds of data stores that can be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those types of systems.

So, we use relational database management systems (RDBMS) to store and manage huge volume of data. This is called a relational database because all the data is stored into different tables and relations are established using primary keys or other keys known as foreign keys.

The PHP language has been developed in the early fall of 1994 by Rasmus Lerdorf. This scripting language allowed him to keep track of users coming to consult his CV on his website, through access to a SQL database queries, in 1995 Rasmus Lerdorf put online the first version of the program which he called Personal Home Page Tools, then Personal Home Page v1.0.

Due to the success of PHP 1.0, Rasmus Lerdorf decided to improve the language by incorporating more advanced structures such as loops, conditionals, and there joined a package to interpret the forms that had developed as well as support for MySQL

In 1997, Zeev and Andi Suraski Gurman joined Rasmus to form a team of programmers to develop PHP 3. Stig Bakken, Shane Caraveo and Jim Winstead joined them later. Thus the version of PHP 3.0 was available June 6, 1998. At the end of 1999, version 4.0 of PHP, PHP4, appeared. PHP is now in its fifth version.

4 SHOPPING CART TECHNOLOGY

4.1 Overview

The Shopping Cart is used by consumers to purchase products or services over the Internet. Usually, it is technically a simple web application featuring the information about the products or services and bearing an integrated purchase ordering and payment processing system. Its information can be stored in a database using MySQL and all the information handling can be performed by using PHP. Nevertheless, shopping cart is not restricted to these two technologies only. It is a very extensible application. A sample shopping cart is shown in Figure 2.2.

Figure 2.2 Sample of shopping cart

4.2 Features of a good Shopping Cart

There are many types of shopping carts in use in the market integrated with many features. A commercially deployed shopping cart should have at least the following features in the following categories in order to achieve the best results for the business:

4.2.1 Customer Service Perspective

- All orders should be stored in the database
- Customers should be able to search and browse personal order history
- Automated confirmation emails system
- Password reminder for customers
- "Send to friend" section for sharing
- Newsletter management
- Printable invoices
- Ability to change the order of products on the customer side

4.2.2 Payment Gateways and Methods

- Acceptance of payments in multiple currencies
- Allowing payment via several online payment modules

4.2.3 Sales Analysis and Tracking Comprehensive statistics:

- Number of orders display
- Number of customers display
- Product views display
- Category views display
- Sales by product / best sellers sorting
- Detailed Sales report generation
- Searchable order data
- Printable shipping labels
- Export facility for sales and customer data for use in a spreadsheet
- Export facility for orders to quick books format

4.2.4 Sales Reporting and Analysis

- Comprehenssive Sales reporting options
- Product cost vs. sales price
- Search query reports
- Total sales by payment type
- Total shipping charges
- Best seller reports
- Sales by customer report

4.2.5 Search Engine Friendly

- Pages should easily be indexed by all major search engines
- Define custom META tags for every category
- Auto-generated static HTML catalogue
- Search engine optimization options

4.2.6 Database and Platform Compatibility

- Support for UNIX/Linux, Windows servers
- Powered by MySQL database
- Payment processing modules for all major gateways
- Flexible implementation

4.2.7 For recurring Customer Accommodation

- All customer's data should be stored in database
- Greet regular visitors
- Registered customers do not have to enter their data again
- Registered customers should be able edit their profile
- Registered customers should be able to access the history of their orders
- Built-in newsletter engine
- Real-time order tracking for registered customers

4.2.8 Web-based control panel for administration

- Password-protected administrative access
- All changes should be real-time
- Should be able to control the cart from a web browser
- Unlimited number of administrative accounts

4.2.9 Security

- Full HTTPS/SSL support
- Secure HTTPS/SSL administrative access
- Password-protected administrative access
- Encrypted customer data

4.2.10 System Infrastructure

- PHP
- Linux Server
- MYSQL Database

Integration of services and applications in the Shopping Cart technology and extending its features could result in the building of more advance systems such as Enterprise Resource Planning (ERP) and Customer Relationship Management(CRM)., Enterprise Resource Planning is primarily an integration of business management practices through software, web applications and modern e-business technologies. Integrating Information Technology as a whole with regular business process reduces huge costs and benefits a corporate house by streamlining the services in many ways. Similarly, CRM is a system which is built upon various applications and services to handle all customer service activities which includes sales and marketing. A Shopping Cart can work as an honest component of both of these systems.

An advanced Shopping Cart or an integrated e-commerce suite can be developed using some Open Source tools and technologies.

5 MySQL, PHP and WAMP

5.1 MYSQL

MySQL is a Database Management System for multi-users and high-performance, which has become the standard in the establishment of database applications on the Web or outside as illustrated in Figure 6.1.

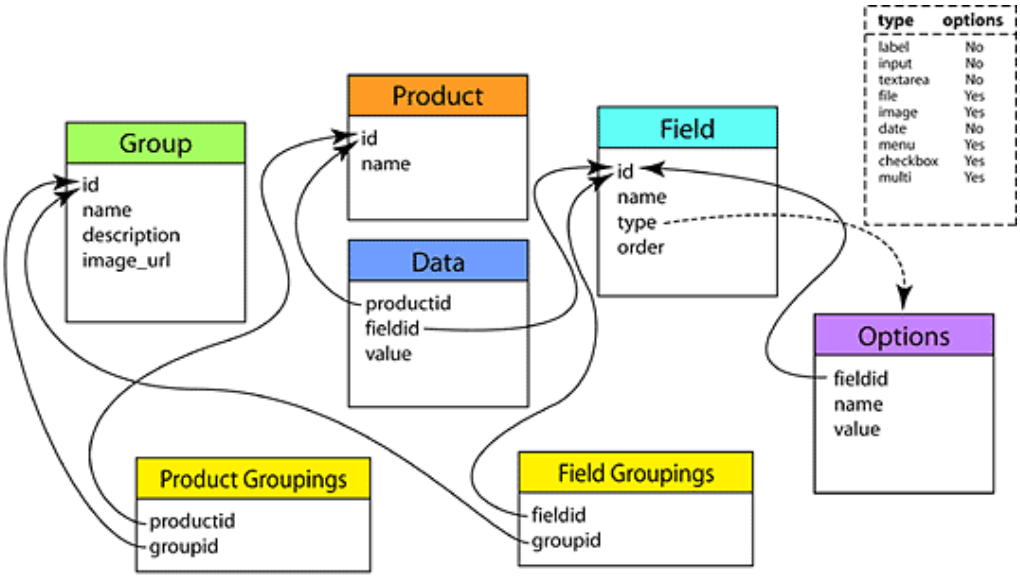


Figure 5.1.1 MySQL schema [12]

MySQL is designed around three key concepts that are: speed, stability, ease of use and, in addition, it is available under an Open Source license, GUN GPL. But the greatest drawbacks of MySQL is the lack of Stored Procedures and transactions and being Open Source does not necessarily mean that is also free of charge, because an Open Source program can be free once it is limited in small project which do not provide any income. The free version is the least power. The strongest versions must be paid an amount.

5.2 PHP

PHP is a programming language and its primary area is the Web applications. What distinguishes it from others programming languages is that it is free and Open Source and it is the perfect choice for web programmers in the world. According to Vyom Munjaal, [5] who is the author of “The Most Popular Web Programming Language”, PHP is characterized by the following characteristics:

- Usability

PHP is one of the easiest programming languages that dispels all complexities of memory management and word processing in C, on the one hand, and a lot of designs of the Perl programming language, on the other hand. The PHP structure very clear; most of the grammar is taken from both C and Java and Perl for the manufacturing of the programming language. It is easy and smooth without losing any strength in the language.

- Speed

PHP is known for its high speed in the implementation of programs, especially in version IV. PHP was originally designed as a nucleus of an interpreter, so that this nucleus can be put in a number of templates or casings to work with different techniques; an interpreter PHP can be run as a CGI, for example. However, the best PHP feature is the possibility of installing an interpreter PHP provider IIS in the form of additional units added to the provider through the functions, ISAPI, and there is another copy of it to ride the provider Apache also in the form of an outdoor unit.

There is also a version intended for integration with the blade equipped with Apache. So that part of the Apache itself which is now the most widely used in Web servers that run on UNIX systems. The blade equipped with Apache gives the best performance when it becomes the interpreter part of the supplier. Therefore it will be loaded in memory waiting for PHP pages to be translated. It is displayed to visitors directly without additional delay required by the programs such as Perl / CGI for example, which must be running an interpreter Perl with each visit to the page translate the page, and then close the translator, then call it up again on the second visit, and so on.

Therefore, Apache Blade would make a difference in major sites of high pressure in particular, and the use of PHP Solution is much better.

- Features

PHP comes with an interpreter loaded with a vast number of functions ready for use in all areas. There is also a set of functions for processing XML, and other functions for sending and receiving files remotely using the FTP protocol, and there is a set of functions for processing and producing images and Flash files dynamically.

- Compatibility

As previously mentioned, although there are plenty of copies of PHP that work in different environments, they all share the nucleus of origin for PHP files, so all the translators PHP behave the same way with regard to the implementation of the scripts. If the script is running on a Windows system with its IIS (Internet Information Server), it should work without the need for any changes. In addition, the changes that have occurred in the previous version exist in the infrastructure of the translator.

- Security

PHP provides a lot of advanced features but gives the appropriate ways to set limits on these benefits. The PHP settings file controlled by the site manager can perform the following functions: controlling the number of contacts allowed to the database instance or the maximum size of files sent through the browser, or allowing the use of some features or eliminating their use

- Scalability

Users can expand the interpreter PHP easily by adding features such as the language C, and where that code of the translator is open, changes to obtain the suitable version from the translator can be implemented. In addition, users can also work with additional units mounted on the compiler to increase the

features and functions built-in such as access to databases and processing XML. The PHP development team has already translated the work of this task and the transfer of huge amount of libraries written in C to custom libraries has been added to the interpreter.

5.3 WAMP

Local server Windows Apache MySQL PHP (WAMP): PHP requires that server software be running on the computer in order to display these types of files on the Web browser

For this thesis, WAMP was used as a local server because it is fairly easy to use, very fast when changing versions for testing and more flexible when it comes to development.

6 SECURITY AND ENCRYPTION

6.1 Security issues

Security threats are experienced in e-commerce due to its nature. The ever growing nature of e-business activities are accompanied by security attacks which can be network attacks, exploitation of vulnerability, availability attacks. For example, the vulnerability in third party software, like Shopping Cart can be exploited. Since it involves business transactions, it may be a very lucrative field of attack. Financial and personal information may be misused after being intercepted when those data transverses through the internet. As there are growing security threats in E-commerce, hence the security concern arises on par with threats. Web security can be classified on the basis of the location of the threat. It can be on the server side, the client side and the network traffic in between the server and the client.

A message is vulnerable to attack on its way from source to destination, and hence network security is the most important factor in e-Commerce activity. Different measures are implemented to achieve confidentiality, authentication, availability, non-repudiation and integrity of the message which are the fundamental parts of the information security.
Server side security is also to be maintained as this creates trust and secures the most important data which is kept in central location. The service offered by the server should be available when the customers want to access it. The physical security of the server is also the prior concern and responsibility of the merchant. There can be vulnerabilities in DBMS, buffer overflow attack, and insecure scripts which can severely downgrade the security of server and hence services.

Information security in E-commerce is all about maintaining public trust, which appears to be more a business issue rather than a technological issue. But here in this paper, we focus on the technical aspects of security which is achieved by using cryptography. In E-Commerce activities, the cryptographic approach provides a solution to transaction side security issues only.

6.2 Cryptographic Technology

To run a business in a secure and trustful manner, the business needs to fulfill some requirements for the purpose of achieving security and trust especially in e-Commerce activities. Since, the message in between the client and the merchant passes through an insecure public network, there should be some mechanism to ensure security and trust. What are those business requirements which should be fulfilled? How can we fulfill those requirements with cryptographic technology? These issues are really advanced to discuss in detail, but we are going to introduce them in brief.
The business requirements necessary for e-commerce activities are outlined and explained below:

6.2.1 Message Confidentiality

Since the message should be confidential when it passes across the network, confidentiality is maintained by implementing an encryption mechanism. Confidentiality assures that the meaningful message is only shared among the intended parties; here the term ‘meaningful’ does mean that the message is not understood by all other parties. So, it is all about maintaining privacy in broader view. In this way, the client is assured for the safe transfer of their payment and payment-related information.

6.2.2 Message Authentication

Authentication verifies the parties involved in the communication, and proves that they are who they claim to be. In the case of e-commerce, the identity of the merchant and the client should be ensured. So, authentication establishes trust in between the communicating parties and ensures that the message is originated from the intended parties.

6.2.3 Message Integrity

Integrity assures that the message is not altered on its way from source to destination. In case of e-commerce activities, it assures that the transaction-related information is not altered on its way in through an insecure public network. The receiver can identify if there is any change in the received message. Any data which is changed during transmission can be dropped instead of further processing.

These requirements basically arise as a consequence of the new platform of the business. Doing business in totally a different platform, the Internet, is really a great challenge in terms of security. But, as a result of a growing concern about network security, there is more trust in e-commerce activities. A server side attack is still a threat, a DoS attack can render the availability of service, and a disgruntled employee can leak out the business secret; but there are secure cryptographic implementations to ensure network security achieving confidentiality, integrity, and authenticity of the message. Due to the implementation of cryptographic technology in the SET (Secure Electronic Transaction) protocol, neither the merchant nor the customer can commit fraud against each other. The cryptographic technology implemented to assure the above mentioned business requirements are briefly discussed in the following sections.

6.3 Encryption

Encryption is the process of converting a readable plain text into so called unreadable cipher text. Symmetric encryption and asymmetric encryption are the two encryption techniques which use mathematical algorithms to convert plain text message into cipher text message and vice versa. Encryption itself assures message confidentiality by hiding the real message, but symmetric encryption is used for message confidentiality in general. Before proceeding to discuss about how we achieve

message confidentiality, let us review how symmetric encryption differs from asymmetric encryption.

6.3.1 Symmetric Encryption

The symmetric key algorithm uses the same shared-secret for both encryption and decryption of a message. As shown in f Figure 6.3.1.1 below, unencrypted source message is encrypted with a shared-secret key which is possessed by both sender and receiver. The encrypted message is communicated to the end user (receiver) which decrypts the message with the same shared-secret key and the message is revealed in its unencrypted form.

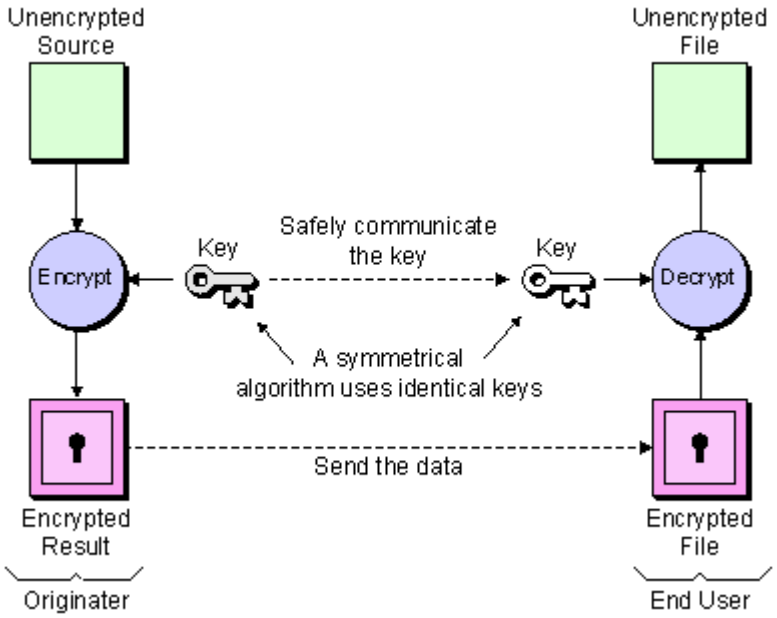


Figure 6.3.1.1 Symmetric key algorithm [13]

DES (Data Encryption Standard), 3DES (Triple DES), IDEA (International Data Encryption Algorithm) and AES (Advanced Encryption Standard) are some examples of the Symmetric Encryption algorithm.

The computational requirements for symmetric encryption are comparatively lower than that of asymmetric encryption, which has the advantage of higher speed. Both encryption and decryption for even larger files take less than a second in a modern computer. So, the large chunk of messages is encrypted with symmetric encryption

techniques. A cipher such as DES (*qv*) will be at least 100 times faster than the asymmetric cipher RSA in software implementation and might be up to 10,000 times faster when implemented on special hardware. However, the key distribution is more challenging in this technique than in the asymmetric encryption technique.

6.3.2 Asymmetric Encryption

The asymmetric encryption algorithm (Public-key cryptography) uses two keys: - public-key and private-key. The message encrypted with one key can be decrypted with another key and vice versa. For example, RSA and ECC are asymmetric encryption techniques.

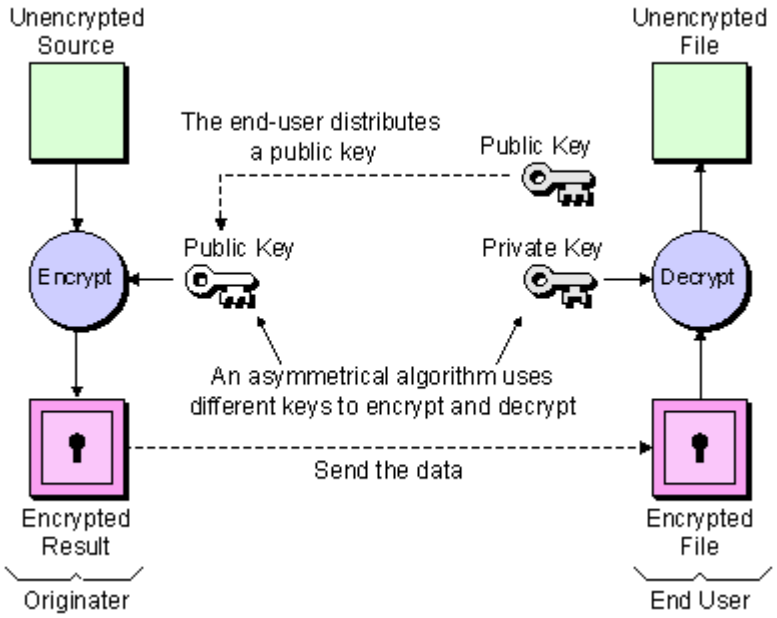


Figure 6.3.2.1 Asymmetric encryption [14]

The public-key of the sender is made available to everyone who is involved in communication, but the private-key is kept secret. The message encrypted with the public-key can be decrypted with the private key of the receiver.

Public-key cryptography is more secure, and it is harder to crack than the symmetric techniques with equal key sizes. The private-key is kept secret and no one knows the key except for the owner itself. On the other hand, its high computational requirements make it slower than the symmetric encryption techniques. A large block of data may

take hours for encryption and decryption. Furthermore, asymmetric encryption techniques are difficult to configure and more difficult to use than symmetric encryption. Both symmetric and asymmetric encryption can be implemented together, and that can be referred to as hybrid encryption. In general, a more practical approach of creating secure communication is with the implementation of both symmetric and asymmetric encryption techniques which nullifies the drawbacks of each technique.
As already mentioned, confidentiality is achieved by encrypting the plain text. The very nature of Symmetric Encryption is a good choice for maintaining confidentiality in spite of its difficulty in key distribution. Brute force, an attempt to break the key using all possible bit arrangements, is only an effective attack for any algorithm. So, the key space determines the security of the algorithm. Hence, due to the greater speed of symmetric encryption technique; it is implemented for maintaining confidentiality in general. The shared-secret key can be both permanent and temporary for only the established session.

6.4 Message Integrity Assurance

In e-commerce, it is very important that the data is not changed during its transmission. There may be eavesdroppers hearing in the network to catch the network traffic carrying transaction data, and they can alter the data to change the transaction details for their benefit. Competitors in business can modify the data to degrade the business reputation. So, the message should be verified so that there is no change during the transmission period and here comes the role of message integrity.

Message integrity can be achieved in many ways. The hash function can check the message integrity. There are several hash algorithms like MD5, SHA1 etc. Digital signatures can provide both message integrity and authentication. HMAC uses one of the hash algorithms and a shared-secret key to provide both authentication and message integrity.
We will discuss about the hash function in general next. Digital signature is discussed in depth in the message authentication section.

Hash Function: As an alternative of MAC, hash is a one-way function which accepts variable-size message M as input to produce a fixed length output message digest H

(M) where H is the one way hash function. Unlike the MAC, it does not include a shared-secret key as input.
Hash function requirements: The fingerprint of file is produced with hash function. To meet the security requirements, hash function H should meet the following criteria:

- H can be applied for variable lengths block of data. So, the input may have any length of data; but always produces the same length of output whatever may be the input length.
- The output of the function should be easily computable making hardware and software implementations easier.
- The hash function should be one way, i.e., there should be no inverse of the hash function so that it is computationally unfeasible to find out the input message just by knowing the value of hash. It helps to keep message confidential, otherwise it does not matter whether the message is encrypted or not but can be revealed with hash output values.
- The hash function should be collision-resistant so that no two inputs should have the same output, i.e., the fingerprint of each file should be unique and distinct.

6.5 Cryptography and Message Authentication

Encryption is enough to protect data from eavesdroppers assuming that the shared-secret key is only known by two parties in symmetric encryption techniques and private-key is only known by the owner in asymmetric encryption techniques. But how can we prevent the falsification of data and transactions? How does a client believe that the website receiving his transaction related information is not set up by attackers posing as the e-merchant? How can we assure that the data is authentic? As an involved party in business transaction, the merchant and the customer wish their data to be authentic, i.e., it should be genuine and should come from the alleged source and here comes the role of cryptographic techniques for message authentication.

Authentication can be achieved in two ways:

6.5.1 Message authentication with conventional encryption techniques

Only the genuine sender and the genuine receiver share the shared-secret key in the conventional encryption system. So, the message can be encrypted and decrypted only by them. Furthermore, the message can embed error detection code, nonce, and sequence number to assure receivers that no alternations have been there in the message during its transmission.

6.5.2 Message authentication without message encryption

It is possible that, even without message encryption, there are cryptographic solutions to achieve message authentication. In general, the message is passed through some procedures and a message authentication tag is generated and appended to the message. The message itself is not encrypted, so it can be read by the destination and is independent of the algorithm used by the sender and the receiver for the purpose of generating a message authentication tag. Since conventional encryption techniques provide both authentication and confidentiality, this approach is preferable when: -

i) When the same message is to be broadcast to several destinations, this approach is more preferable. The message can be authenticated only by one of the receivers, which reduces the computational load in the network. If a message or packet is not authenticated, the responsible receiver can notify other receivers of it.

ii) If the receiver is running a heavy load beside, then the decryption of all messages authenticated with conventional encryption system seems to be deteriorating the condition further. So, this option is preferable in that situation.

iii) Authentication of several computer programs in plain text enable the execution of a computer program without decryption of code every time. But, if the message authentication tag is appended instead; it can be checked randomly anytime at a preferable time during the execution of program.

The first method approaches ensures authentication and confidentiality by encrypting all the message and hence consuming system resources greatly, and the second method approaches only provides authentication with a low overhead on system resources. So, are there any best alternatives which assure both confidentiality and authenticity with low system overhead and high speed?

Before proceeding to the solution of this problem, message authentication code and public-key cryptography will be introduced. Public-key cryptography will be discussed in more detail before delving into digital signatures, a way for authenticating two parties involved in communication.

6.5.3 Message Authentication Code

Message Authentication Code, MAC, a small block of data, is generated using a secret key and appended in message. If we assume that Alice and Bob are communicating with each other and their secret key is KAB. Suppose Alice has message M to be sent to Bob, then Alice passes the message M and key KAB to the hash function F. The Figure 6.5.3.1 below displays the message authentication code techniques: -

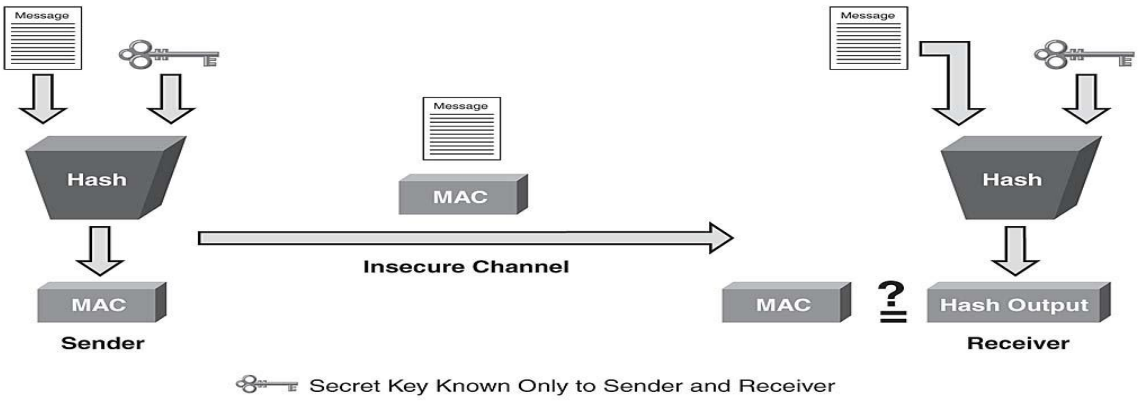


Figure 6.5.3.1 message authentication [15]

Hence message authentication code MACAB = F (KAB, M) is calculated. The appended MACAB is sent to Bob along with message M. Since Bob has the same secret key KAB and Bob passes the received message and the secret key through the same function F. So, the Message Authentication Code calculated by Bob will be: -
MACBA = F (KAB, M).
If MACBA = MACAB, then the message is supposed to be not altered and is, therefore, authentic. If the message is altered, then the calculated MACAB should be different to MACBA. And the message is authentic since the share secret key is only known by the sender and receiver.

6.5.4 Public Key Cryptography

The public-key cryptographic technique has the following ingredients:

a) Plain text: It is a readable message, an input to public-key cryptographic encryption algorithm.

b) Encryption algorithm: It performs various transformations in input message to produce cipher text.

c) Public and Private Key: They are interchangeable; if one is used for encryption, then the other can be used for decryption. The public key is made public and available to all other parties which are involved in communication, but the private key is kept secret and known by the owner only.

d) Cipher text: It is a scrambled message, an output of the public-key cryptographic decryption algorithm.

e) Decryption Algorithm: The cipher text is fed as input along with the proper key, which produces plain text as output.

6.5.5 Essential steps in public-key cryptography

a) Two parties generate a pair of keys, i.e., public-key and private-key. Let A and B be two users involved in communication.

b) Suppose that the public-key and private-key of A are PUa and PRa respectively, and the public-key and private-key of B are PUb and PRb, respectively. Then, PUa and PUb are available to each other by any ways.

c) If A wishes to send a message to B, then there are two options for A:

- A can encrypt the plain text message with the public-key of B (PUb), so that B can decrypt the cipher text message with its own private-key (PRb).
- A can encrypt the plain text message with its own private-key (PRa), so that B can decrypt the cipher text message with the public-key of A (PUa).

d) B decrypts the message of A either with PUa or PRb depending on the choice of key by A. Since Public-key and Private-key are exchangeable, it is possible to use either of them for encryption so that they can be used in pairs for encryption and decryption.

Mathematically, Diffie and Hellman postulated the requirements for public-key cryptography. According to them [11], public-key cryptography should meet the following requirements:

1) For party A, its public-key PUa and private-key PRa should be easily generated computationally.

2) For Party B, cipher text C should be easily generated by encrypting message M with PUb.

I.e., C = E (PUa, M) should be easily generated, where E is the encryption algorithm.

3) The receiver B should be easily able to compute the plain text message by decrypting the cipher text message with PRb; i.e. M = D(PRa, C) = D[PRa,E(PUa,M)]

4) PRa should be computationally unfeasible by knowing PUa only.

5) Knowing PUa and C only, it should be computationally unfeasible to decrypt C.

6) Either of the two related keys can be used for encryption provided that the other pair can be used for decryption. So, it should be possible to proceed like: -

$$M = D[PUa,E(PRa,M)] = D[PRa,E(PUa,M)].$$

6.5.6 Digital Signatures

Authenticity and integrity are achieved by digital signatures. Indeed, a digital signature is a mechanism which verifies who the sender is. For example, suppose A is sending a message M to B. Before the message exchange occurs, sender A distributes its public-key (PUa) to B. Then the whole message to be sent is encrypted with the private-key of A (PRa).

So, the encrypted message ciphertext C = E(PRa,M).

Now the scrambled message is decrypted by B using the public-key of A (PUa).

So, M = D(PUa,C) = D[PUa,E(PRa,M)]

Now the message can be decrypted only by the public-key of A, but not by others. So, the receiver B is assured now that the sender is A. So, the whole message is a digital signature. But encrypting the whole message is computationally resource-consuming. So, is there any other alternative?

A better way is to encrypt the blueprint of a file, which is the small representation of the file. As mentioned in hash function, the message digest is the blueprint of a file which

has the property that it is unfeasible to have different documents without having different blueprints. The blueprint of the whole message is called authenticator, which is encrypted with the private-key of the sender. The encrypted content now serves as a digital signature. A secure hash code such as SHA-1 and MD5 serve as the function which generates the authenticator.

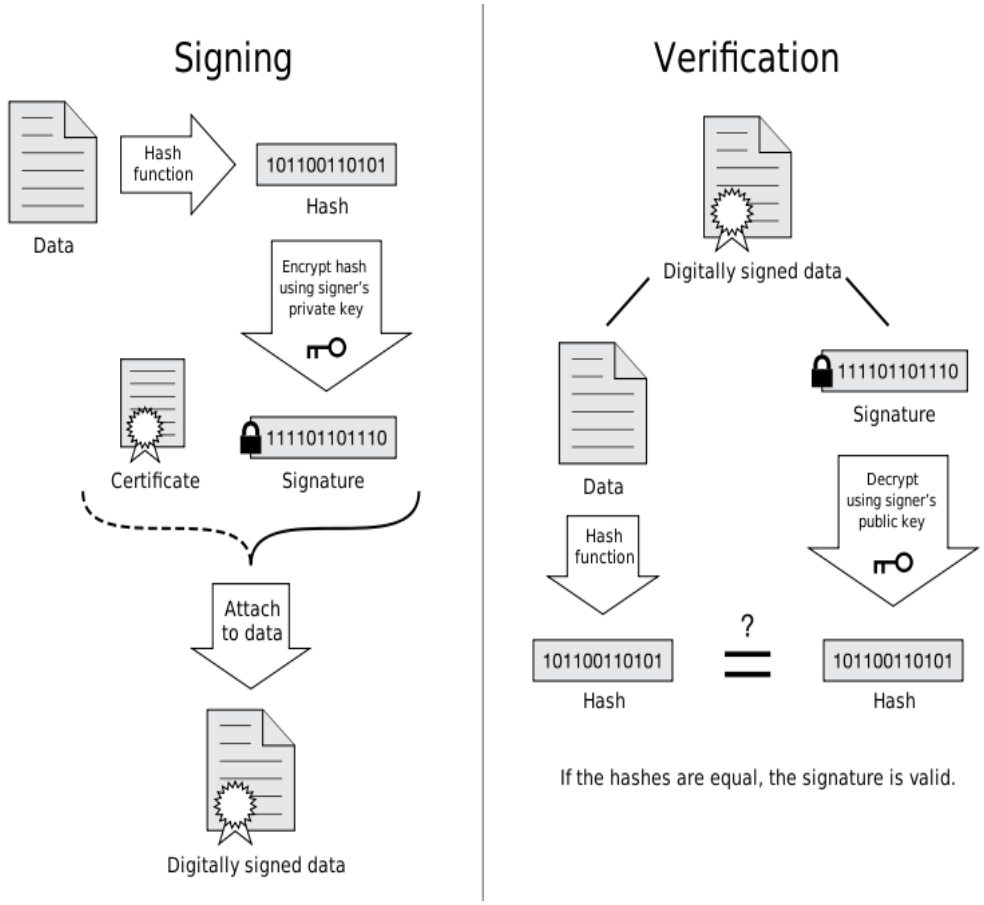


Figure 6.5.6.1 Digital Signatures [16]

As shown in Figure 6.5.6.1, the data is passed through the hash function and a fixed length hash key is generated. The private-key of the sender is used to encrypt the hash key, which is appended to the original data. Then, the appended data is digitally signed and transmitted to the receiver. When the receiver receives the digitally signed data, it passes only the data through the hash function separating the signature for decryption. The signature is decrypted with the public-key of the sender, which reveals the hash key generated by the sender as discussed in the public-key cryptography section previously. The message is sent through the same hash function in the receiver and

the hash key is generated as a result. If the hash key calculated in the receiver side is the same as the hash key sent by the sender, then the message is not changed on its way from sender to receiver. So, the message integrity is checked. Now, the message is also authenticated. Since the decryption of the digital signature appended with the data is only possible with the public-key of sender, there is no other sender except the sender itself. If there is a change in the message on its way from source to destination, then two values of the hash key should not be same. In rare cases, a trustful third party agency timestamps the message to provide non-repudiation.

Message authentication is secured by Public-key Certificates:
1.Message authentication is achieved by conventional encryption or /with public-key encryption.
2. H They checks the digital certificate. This is a digital document issued by the CA (Certification Authority: VeriSign, Thawed, etc.) that uniquely identifies the merchant. Digital certificates are sold for emails, e-merchants and web-servers.

6.6 Security Measures

Confidentiality, authentication and integrity are also discussed here.
1. Securing the network:
The network should be kept secure for maintaining confidentiality.
2. Securing the server:
The merchant should be responsible for providing server side security in e-commerce activity. In minimum, the server should be secured with firewall and anti-virus software tools. If customer data is to be kept safe, then keeping back-ups is also the merchant's responsibility.

- The availability of the service offered by merchant should be guaranteed. There may be DoS attack which prevents the potential customer from accessing the service offered. This can downgrade the prestige of the business.
- The database should be secured. Users should be provided with the minimum privilege required to perform only the action needed. SQL injection should be avoided.
- Remote command execution attack is also probable.

SET uses public key infrastructure to maintain privacy, and the merchant, the customer and the bank are authenticated with digital certificates which are issued by the

Certificate Authority. This approach creates an atmosphere of trust between the customer and the seller.

Although credit card details are sent in encrypted form with SSL, it does not guarantee the security of client against possible fraud of the seller. SET ensures that the precious and sensitive information is not revealed by the merchant. The information received by the merchant is not stored in the merchant's server, which is secured by using nonce.

7 Case Study: Movie Gallery

Movie Gallery was the Shopping Cart which the author designed using PHP Scripting language with MySQL database. Although it was a starter project, it had a lot of advanced features provided by those Open Source tools. Below is an overview of the project.

7.1. Some Screen-shots

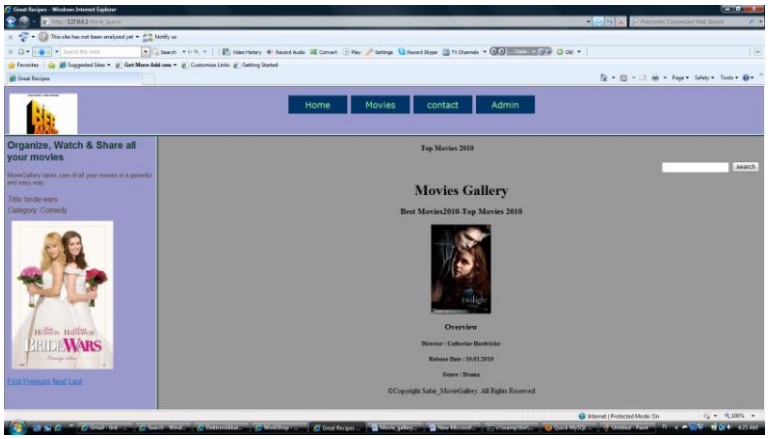


Figure 6.5.6.1 Digital Signatures

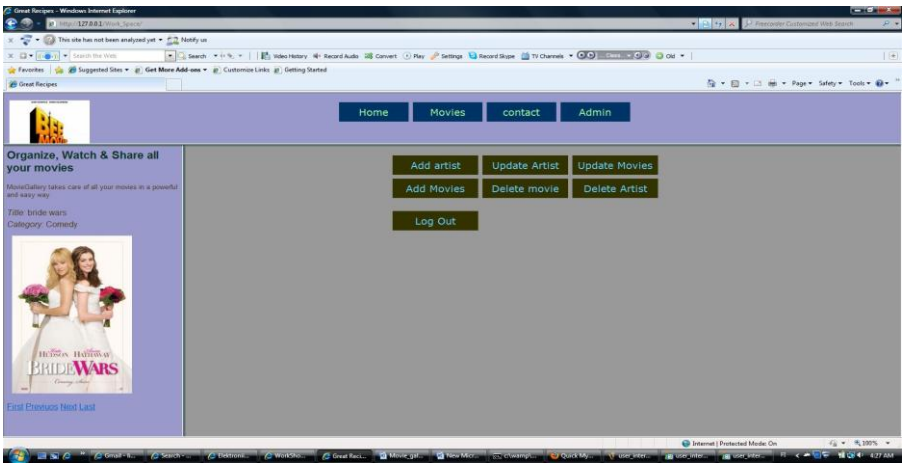


Figure 7.1.2 Selecting Movies

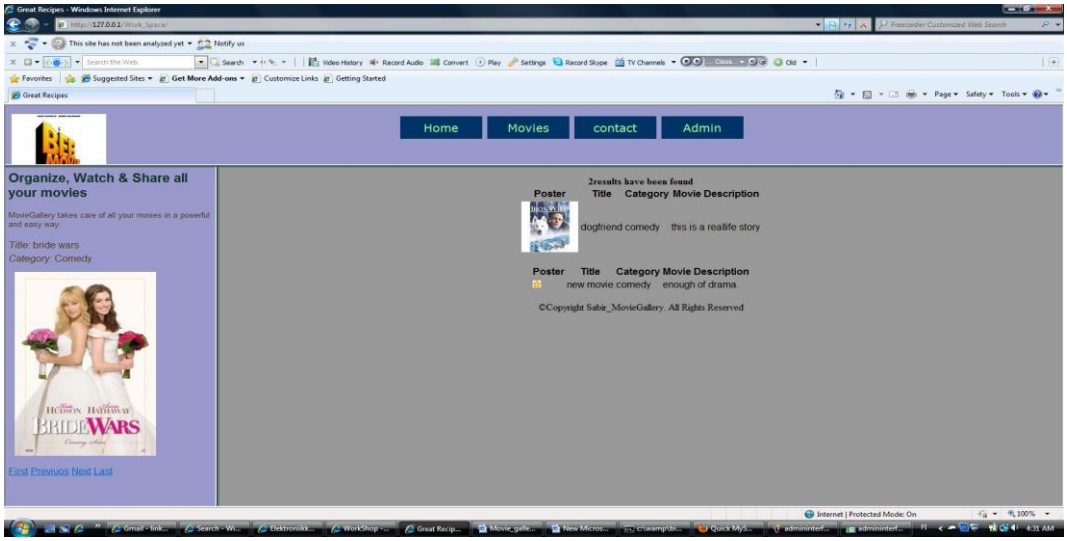


Figure 7.1.3 Updating Data

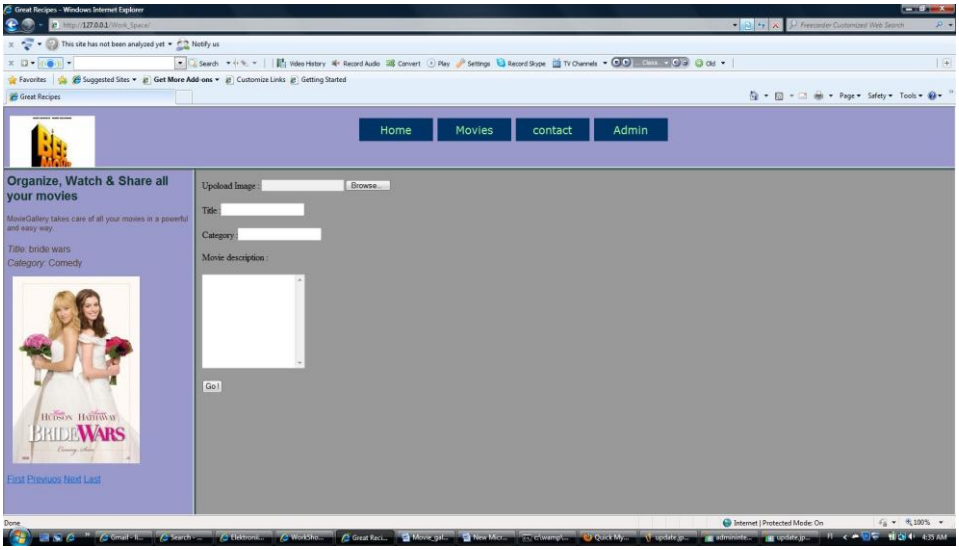


Figure 7.1.4 Form

7.2. Movie Gallery Features

Stored Procedures

The stored procedures method was used to create a sub-routine to applications accessing the Movie Gallery database system. It allows the results of a select statement to be processed using cursors for other stored procedures by associating a result set locater, or by applications. It also allows variables to be received and returned, depending on how and where the variable is declared. We stored our data on the Apache server. This was done using the PHP script of insert. The insert command stores the data into the database and this can be demonstrated by using the select stored data from any tables in our project's database. Using the SQL syntax : SELECT * FROM table_name WHERE…(and here come the roll of foreign keys in the roll table), enables us to retrieve data from both tables (movie and artist) using the foreign keys *movieCode* int unsigned, *artistId* int unsigned which are primary keys in the movie and artist tables.

Trigger

This allows the Movie Gallery database to be executed automatically in response to certain events on a particular table or view, so as to keep the integrity of information on the database. It enables users to cancel a requested operation, insert, update, and delete events.

Backup

Copies of data were made so that it can be used to restore the original copy in case of data loss event. Also, a default storage data table called backup was created. In case of any failure of the server, the data will be in the third table. For backup purposes we first installed ZRM for MySQL locally, on a MySQL Database Server.

Then, we configured ZRM for MySQL to perform a backup and we chose to retain our backups for 10 days:

Retention-policy=10D

Data Maintenance

The data maintenance was designed so that it allows the administrator to add, delete, change, and update files. The data maintenance is performed manually and it also backs up, stores and generally keeps up all the data in the database.

User Rights

Only the administrator has the right to delete, upload, and create tables. The normal user can only read and search for information in the database by using a search keyword. The user rights also permit the administrator to focus on rights associated with sensitive data and identify excessive or dormant rights.

Index File

The Index file helps the data on the database to improve the speed of data retrieval operations on the database so that, movie files can easily be retrieved or manipulated.

User Interface

The user interface helps users to create a query that specifies the data to be retrieved from the Movie Gallery database server. With the user interface, we were able to build an SQL SELECT statement that specifies the database tables and columns from which to retrieve data for a report dataset.

Table 1 Movie Gallery Components

File name	Description
admin_movie_add.php	Administration screens to add a movie record.
admin_movie_edit.php	Administration screens to edit or delete an existing movie record.
admin_movie_list.php	Administration screens to display a list of the movies in the inventory.
admin_artist_add.php	Administration screens to add a new artist.
admin_artist_edit.php	Administration screens to edit or delete an existing artist record.
admin_artist_list.php	Administration screens with a list of all the artists.
admin_footer.php	Footer for all administration pages.
admin_header.php	Header included on all the administration pages to provide a connection to the database, to check if the administrator has logged in or not, and to provide the administration menu.
admin_login.php	A login screen to verify the username and password entered and to update the session so that the user can freely use the administration pages.
add_admin.php	Administration screens to add and edit a new administrator.
artist_detail.php	A public page to display all the information for a specific artist.
contact.php	A simple public form to request contact with the staff. This form sends an email when submitted.
search.php	A public page to allow the user to search by movie title, artist name, or by the specific category.
footer.php	The footer that is included at the bottom of every public page.
header.php	A header that is included at the top of every public page to provide the navigation bar, database connectivity, some PHP-specific functions, and the logo.
index.php	The initial page to display the list of all the latest movies.
style.css	A cascading style sheet, used to specify the fonts, color, and so on.

7.3 Shopping Cart Implementation

7.3.1 Overview

The Shopping Cart project was completed using the freely available Open Source tools such as PHP, MYSQL, Firefox, Apache Server (on Windows Operating System), EclipsePt Integrated Development Environment etc. Various issues arising thereafter were handled with proper care and caution in the mock implementation phase of the testing. In addition, switching the data storage method from MySQL database to XML was carried out to suit our needs.

7.3.2 Segments of Movie Gallery

- The Database Back-end

Basically, a MySQL database is used to store all data of the application. But data storage system can be also successfully implemented using XML which has various benefits over the MySQL database. Here, XML works as a DBMS system. The storage, schema, query, programming interfaces etc., are provided by XML although it does not provide more advance features such as triggers, queries, multi-user access that a real database constitutes. The implementation of XML makes the data portable and allows storing data in nested forms.

- The User Interface

There are various components which constitute the user interface of the application. Primarily, there is an HTML document which is read and interpreted by the web browser. This document is the prime skeleton of the application with is styled as defined by another CSS document.

A CSS document, Cascading Style Sheet document, is the document that controls the look and feel of the whole application. It defines the color, position, size and display of the various components from the HTML document which are to be shown in the user interface.

Another component used in the application is the JavaScript which runs on the client side without interacting with the server as soon as the page is loaded. This is used for various purposes such as loading forms and wizards. This decreases the timing of the page loading and refreshments hence improving the performance.

All transactions lodged in the database or storage file are handled by a scripting language which is PHP in this case. PHP is a scripting language that collects commands from the user and makes the intended transaction upon the database. It is interpreted as HTML document by the web server in order to make it readable by the browsers. It also controls the displaying characteristics and it forms as a wrapper around the application. Some kind of PHP script is executed for each type of action. Therefore, this is the main functioning unit of the application.

7.4 How To Prevent Some Possible Threats

Most of web applications that use a database build a command to operate the database based on user input. This means that if the command-building process is not securely guarded, attacking and manipulating the database would become possible. This issue is called “SQL Injection vulnerability” and the attacking method exploiting this vulnerability is called “SQL Injection attack”.

7.4.1 Cross-Site Scripting

This vulnerability could allow malicious attackers to:

- Display a phony web page on the legitimate web site resulting in
  - Confusion caused by false information
  - Disclosure of sensitive information through phishing attacks
- Steal cookies retained by the web browser
  - Personal information stored in the stolen cookie would be disclosed.

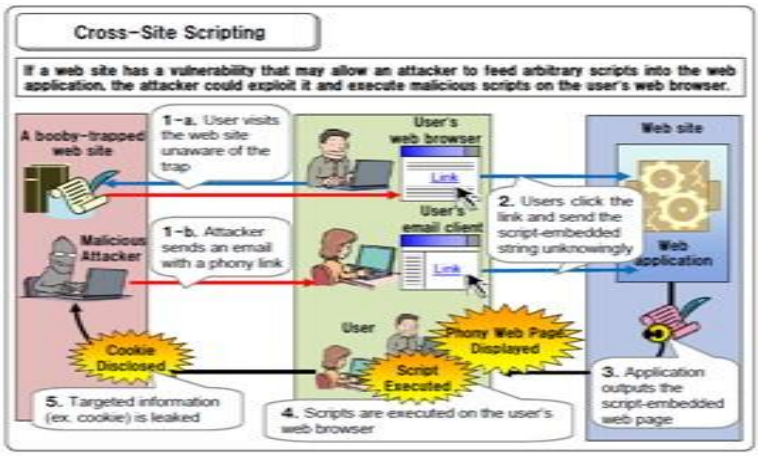


Figure 7.4.1.1Fundamental Solutions in Movie_Gallery[17]

- SQL Injections

  The most dangerous of Cross-Site Scripting, which works by injecting some query to obtain data such as a password administrator or program manager from database.

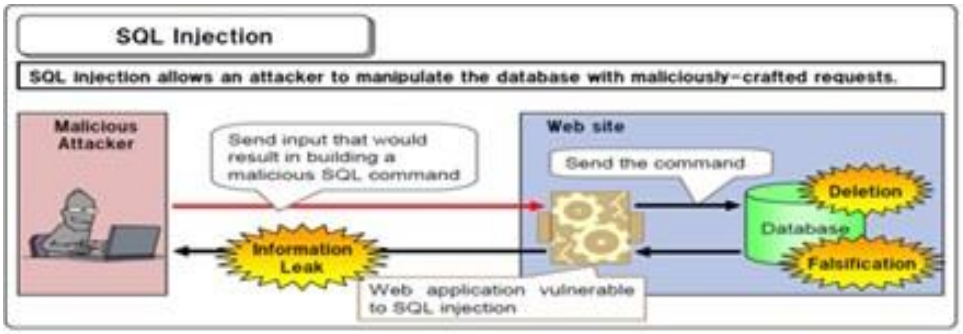


Figure 7.4.1.2 SQL Injection [18]

In our case, in Movie Gallery we have implemented some security measures against SQL injection attacks which are summarized as follows:

- We use the binding mechanism to build SQL statements.

The bind values are ‘escaped’ which prevents a malicious attacker from building and executing an ill-intended command.

- We do not allow SQL statement to be directly passed to the web application.

Specifying an SQL statement in a web application parameter directly could lead to a risk of someone falsifying the value of the parameter and manipulating the database parameters, such as hidden, that are to be passed to the web application.

Cross-site-scripting

- We perform Escaping for everything to be output to the web page

  To control the layout of a web page, instead of using characters, such as, “<”, “>” and “&”, we use the HTML entities “<”, “>” and “&” respectively.

- We do not allow the <script> ... </script> tag to be dynamically created based on the external input.

We could check risky scripts but it is would better not to let the application dynamically set the value for the <script> ... </script> tag, for it would be difficult to determine which scripts are indeed dangerous ones for sure.

- We do not allow importing style sheets from arbitrary web sites

Scripts can be written into style sheets using a function like expression (). That means that malicious scripts can be inserted into the web page if the web site design allows to import a style sheet from arbitrary web sites.

- We also perform JavaScript validation

The submit function will call the JavaScript validation to make sure the fields are filled out.

```
onSubmit="return formcheck(this);"
```

7.4.2 Authentication

When a web site needs access control, we implement an authentication mechanism that requires users to enter some kind of secret information, such as password. We also implement authorization as well as authentication to make sure that a login user cannot pretend to be other users and access their data

- Encrypting Password using md5() function

To make the login password more secure, we use the md5 function. The example below shows how it works

Figure 7.4.2.1 Encrypting Password using MD5 [19]

- Server side validation

  - We run the server using an ordinary (unprivileged) login account, not as root.
  - We make the MySQL data directory accessible only to the server account.
  - We require each account to have a non-empty user name and password, avoid use of wildcards in hostname specifiers, and grant only such privileges as are really needed
  - The Apache server is not more secure when we are dealing with large businesses for this reason we have to set up advance configuration instead the default one that has been using during a personal project.

7.4.3 Secure Apache Server

:

A secure Apache Server includes serving other protocols on Apache (POP3) and using SSL on Apache to better secure Web transactions. These options will allow us to expand the range of services offered by the Apache server.

When performing business transactions on the Internet, security is of huge importance.SSL (Secure Socket Layer) is a protocol that implements the Public Key encryption algorithm to provide this security. This protocol allows clients to connect to a Web server across the public Internet with confidence that the traffic between themselves and the server cannot be read by third parties. They can also have confidence that no third party has redirected their traffic from a known, trusted server to a malicious, unknown server. The actual mathematics and cryptography of how this works do not belong to the scope of this thesis.

Conversely, SSL also prevents hackers from impersonating users in communication with servers. It is currently the best system in general use that gives both servers and users confidence that their communication is actually going where they expect it to go and cannot be read, hijacked or mistreated in some way en-route. While SSL was originally designed for use solely on the Web as a security protocol for Internet shopping, it has since seen an extension to many other protocols that send data in plain text over the Internet, including FTP, POP3 and IMAP. Many of these servers now implement an SSL version of their basic protocols that encrypts their data as it leaves

for the Internet and decrypts inbound traffic. Also, with the advent of workplace use of instant messaging for actual business purposes, many Instant messaging (IM) providers have implemented secure features on their protocols as well, based on SSL.

The Apache server required multiple steps of secure configuration, but the most important step that we had to tackle with consideration was the Certificate Signing Request that was sent to the CA for signing and returned as a fully fledged certificate.The following command creates this file:

```
openssl req –new –key myServer.key –out myServer.crt
```

This command takes the key file generated above and uses it to create the myServer.crt file, which contains the certificate request that can be given to the CA through whatever means they wish. This command prompts us to provide more information used to define our organization as a unique unit, including the domain name that is used when connecting to our site. Once we have created this file, we can give it to a trusted CA for them to digitally sign. We can then use the signed certificate to securely process transactions across the Web.

Now that we have our certificate file, we can begin configuring the server to use SSL.The first step is to make sure that we have downloaded and installed the necessary files for mod_ssl and OpenSSL. Once we have these files downloaded, installed and compiled into our Apache server, we will need to configure the appropriate lines in the httpd.conf file.

7.5 XML

7.5.1 OVERVIEW

XML stands for the Extensible Markup Language. It is a markup language for documents, much like HTML, however, XML differs from HTML because it is extensible, meaning that users can define their own tags or other structural aspects of the document, XML allows users to specify the type or form of a document, the elements of a document, the values of those elements, and the relationship of the document and elements to other documents and elements.

.

The following are the key benefits of using XML to store data:

- XML uses human like language which is readable and easily understandable and has a very easy syntax.
- XML is small and portable and compatible with larger Object-Oriented Programming Languages such as Java.
- XML is extendable. It allows creating its own tags specific to any project, defining the attributes of any need, making sense to specific users and programmers.
- It is faster and easier to use in comparably medium and small sized applications.
- It allows the storage of data in application specific pattern very easily because it can store the data in nested forms naturally. Furthermore, the file size is extremely small.

7.5.2 The catalogue (XML File)

We are discussing XML instead of MySQL databases here. Our XML file is catalog.xml which is in very specific format needed for the application. It contains a root item from which some tags and sub tags generate a nested structure. The description of the product is held collectively by this structure in the document as shown below:

```
<?xml version="1.0" encoding="UTF-8"?>

<items>

  <product>

<id>Romance</id>

<title> Letters to Juliet </title>

<description> An American girl discovers a love letter that changes her life in this romantic   comedy.</description>

<img>http://images.fandango.com/r2.1.4//ImageRenderer/94/141/mdcsite/images/global/still_looking94x141.jpg/126401/images/masterrepository/fandango/126401/lettersjulietposter1.jpg</img>

<price>20.00 euros</price>

</product>

</item>
```

7.6 Payment Gateway

Payment Gateway is a very important aspect of the Shopping Cart application as it is the only method to receive the payments. There are many threats and security issues in e-commerce transactions. To minimize such issues, we used the PayPal Service as our payment Gateway. There is a secure connection from the Shopping Cart to the PayPal account and, finally, the Payment Processing Network.

The following steps describe the process of payment processing after a customer inputs credit/debit card information on our on-line Shopping Cart:

- The Payment Gateway encrypts data and securely sends it to the Internet Merchant Account.
- The transaction is reviewed for authorization.
- The result is encrypted and sent back through the payment gateway.
- Results are shown and a decision can be made whether or not to fulfil the order.

Instant Payment Notification (IPN)

IPN is an automated system for order processing. PayPal's IPN is the quick way to obtain results for payment authorizations. The implementation of IPN enables retrieving the information right away on the transfer of money on behalf of the merchant as soon as the sale is closed. A notification receiving the URL or address is specified in the merchant profile at the time of account setup. This information includes the customer's name, payment amount and so on. The whole information is encrypted before sending process so that it is secure and the transaction is only validated after PayPal confirms that the right address received the message.

PayPal is easily integrated with shopping carts. In fact, there are some pre-built commercial shopping cart infrastructures and commercial as well as Open Source shopping cart building frameworks already integrated with PayPal.

8 SUMMARY

The advent of technology brought many benefits along with it. Shopping online looks like the easiest thing we can do when we are in a hurry. There we can shop and we receive our items in less than 24 hours time.

When it comes to payment, somebody can use anyone's credit card when shopping online. A lot of us are concerned about identity theft when we hear about online shopping. Identity theft cases take place in reality in brick and mortar stores and not online. Websites are secure these days with powerful encryption procedures that keep our identity safe and secure. Although there are a few where our information may not be secure, we can take a peaceful breath when dealing with the vast security measures of online shopping websites.

A shopping cart is very flexible and extensive, and can be built using Open Source technologies such as PHP and MySQL. Inspired by its usability, flexibility and simplicity, the author conducted and performed some research work, developed his own shopping cart and presented in this study. In conclusion, E-commerce is now the reliable way to make a business grow. And nowadays, using the shopping cart is a very useful and safe way to buy in the most popular sites on the web by using the SSL certificate system for security and integrity of e-commerce for everyone.

Security issues deriving from the flaws in the software itself go against this ultimate goal. Therefore, it is very important for shopping cart developers to consider security measures and provide tips on how to avoid most common problems.

REFERENCES

[1] Laudon, Kenneth C., Traver, Carol Guercio. E-Commerce 2010: business, technology, society, 6th Ed. 2009. p.100 – 216.

[2] Kamlesh K. Bajaj, Debjani Nag. 2005. E-Commerce: The Cutting Edge of Business. Tata McGraw-Hill. p.10-14.

. Sams Publishing, USA. p. 215-273.

[4] Holden, Greg. 2007. Starting an Online Business for Dummies, 5th Ed. Wiley Publishing Inc, 111 River St., Hoboken, NJ, USA. p.53.

[5] Valade, Janet. 2009. PHP and MySQL for Dummies, 4th Publishing Inc, 111 River St., Hoboken, NJ, USA. p.47.

[6] [www-document] Available at: http://www.apache.org/, consulted: 20.03.2010

[7][www-document] Available at:http://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg, consulted: 24.03.2010

[8] [www-document] Available at: Network http://wwww.networkworld.com/subnets/cisco/102208-ch2-ssl- vpn-technology.html?page=1, consulted: 19.04.2010

[9] Chip Design Magazine, Available at: http://chipdesignmag.com/display.php?articleId=1162, consulted: 14.03.2010

[10] [www-document] Available at http://t3.gstatic.com/images?q=tbn:LXvbA1dkE_iz5M:http://www.designchateau.com/images/featured5.jpg, consulted: 26.04.2010

[11] [www-document] Available at http://chipdesignmag.com/images/idesign/misc/chips040207_figure2.gif, consulted: 20.04.2010

[12]http://www.stationfour.com/images/image-database-schema.png

[13]http://chipdesignmag.com/images/idesign/misc/chips040207_figure2.gif

[14] http://authokeys.com/images/embeded/tools/figure5.gif

[15]http://sslsecure.com/pic/log/misc/145//publicencryption.jepg

[16]http://hkey.com/images/dual/local/chips020475/sign.gif

[17]http://www.ipa.go.jp/security/vuln/vuln_contents/p.15/script.jpg

[18]http://www.ipa.go.jp/security/vuln/vuln_contents/p.21/script.jpg

[19]http://daf.com/privatesol/ides/authonti/publicencryption.gif

APPENDIX

A. PHP code to add artists:

```
File  Edit  View  Tools  Settings  Help
New  Open  Save  Save As  Close  Undo  Redo
<?php
session_start();
require_once 'connect.php';
    $add =(isset($_SESSION['user'])) ? strip_tags($_SESSION['user']) : NULL;
    $submit =(isset($_POST['sabir'])) ? strip_tags($_POST['sabir']) : NULL;

        if($add){

        header('LOCATION:header.php');
        }

        if($submit) {
        header('LOCATION:body.php');
        }

        else {

    $firstname = (isset($_POST['firstname'])) ? $_POST['firstname'] : '';
    $lastname = (isset($_POST['lastname'])) ? $_POST['lastname'] : '';
    $nationality = (isset($_POST['nationality'])) ? $_POST['nationality'] : '';
    $dateOfBirth = (isset($_POST['dateOfBirth'])) ? $_POST['dateOfBirth'] : '';
    $otherInfo = (isset($_POST['otherInfo'])) ? $_POST['otherInfo'] : '';
    if( !empty($firstname) && !empty($lastname) && ($nationality) && ($dateOfBirth) && ($otherInfo)) {
        $sql = 'INSERT INTO artist
                (artistId, firstname, lastname, nationality, dateOfBirth, otherInfo)
                VALUES
                ( NULL, "' . mysql_real_escape_string($firstname,$con) . '",
                "' . mysql_real_escape_string($lastname,$con) . '",
                "' . mysql_real_escape_string($nationality,$con) . '",
                "' . mysql_real_escape_string($dateOfBirth,$con) . '",
                "' . mysql_real_escape_string($otherInfo,$con) . '")';
    mysql_query($sql,$con) or die(mysql_error($con));
    }

    }

?>

</td> </tr>
</td> </tr>
</table>
</td>
<?php
require_once 'footer.php';
?>
```

B. PHP Code to update an artist

File Edit View Tools Settings Help

New Open Save Save As Close Undo Redo

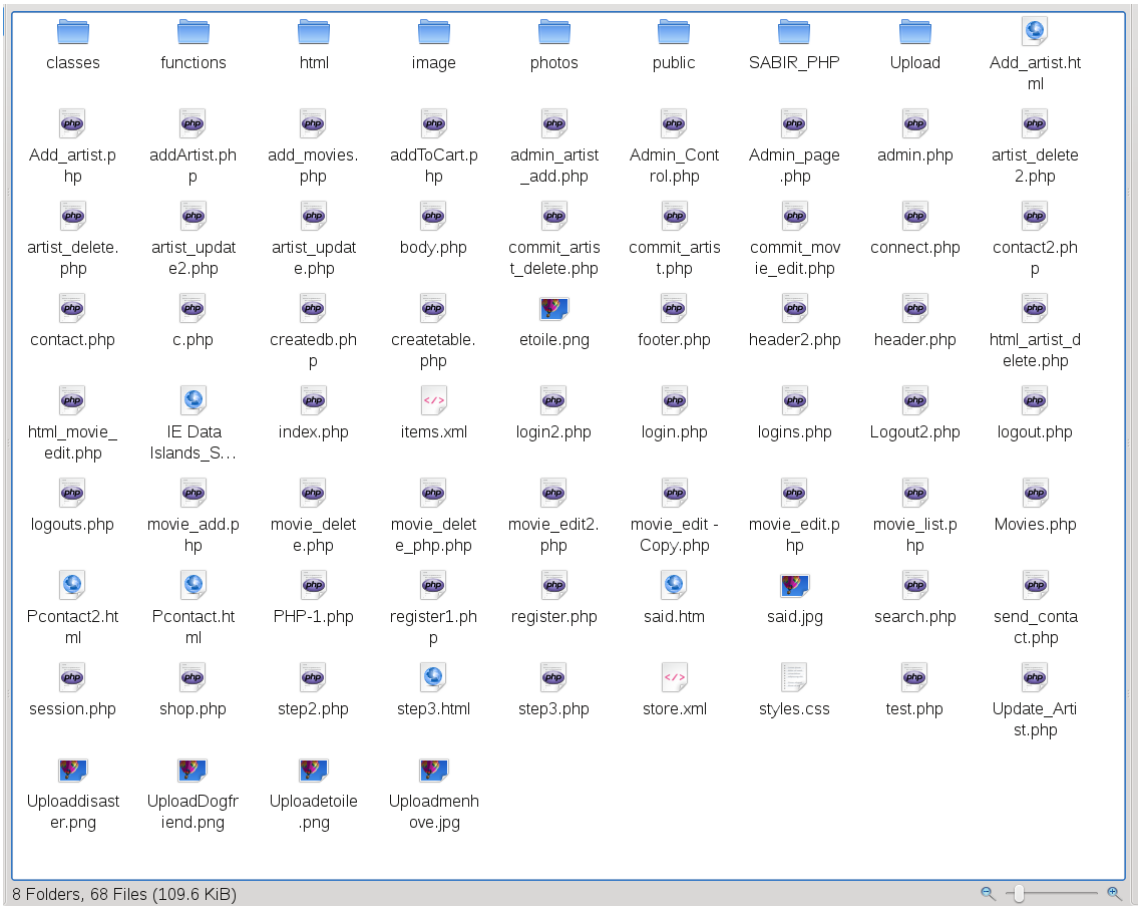
```
background-color:#999999;
}
</style>
</head>
<body>
<table>
<td colspan="8"align="center">   <!--- Body Content  --->
<table width="90%">
<tr> <td>
     <Tr>
          <Td>
<?php
       $query = 'SELECT  artistId, firstName, lastname
                      FROM artist order by firstName';
       $result = mysql_query($query,$con) or die(mysql_error($con));
        if($result < 1) {
          // there are no records to view
          $display_block = "<p> <em> Sorry! No results. </em> </p>";
          } else {
       while ($row = mysql_fetch_assoc($result)) {
          $artistId = $row['artistId'];
          $firstName = $row['firstName'];
          $lastname = $row['lastname'];
          @$option_block .="<option value=\"$artistId\">$firstName, $lastname </option>";
          }

          // create the form block
          echo "<p><img src = \"image/artistimages.jpg\" /></p>";
          $display_block = " <form method=\"post\" action=\"artist_update.php\">
          <p><strong>Artists </strong></p>
          <select name=\"artistId\">
          $option_block
          </select>
          <input type=\"submit\" name=\"submit\" value=\"Select this Artist\"> </p>
          </form>";
       }
?>
<html>
<head>
          <title> Modify a Contact   </title>
</head>
<body>
          <h2> Update Artist Data</h2>

          <p> scoll down to view the hall Artist Lits </p>
          <?php echo "$display_block"; ?>
          <br />
</body>
</html>
</td> </tr>
</td> </tr>
</table>
</td>
```

Line: 58 Col: 1 INS LINE PHP (HTML) Update_Artist.php

C. PHP Code to search the database

```php
<?php
session_start();
include('connect.php');
?>
<html>
<head>
<style>
body {
background-color:#999999;
}
</style>
</head>
<body>
<?php
$button = $_GET['submit'];
$search = $_GET['search'];
if(!$button){
    echo "You didnt submit the search button";
}
    else
    {
        if(strlen($search) <= 2){
            echo "the term of keyword is too short";
        }
        else {
            $explode_search = explode(" ",$search);
            foreach($explode_search as $keyword){
                $x=0;
                $x++;
                if($x == 1)
                $construct = "category LIKE '%$keyword'";
                else
                $construct = "OR category  LIKE '%$keyword'";
            }
            include "connect.php";
            $construct = "SELECT * FROM movie WHERE $construct";
            $results = @mysql_query($construct);
            $found = @mysql_num_rows($results);
            if($found == 0){
            echo "<p><img src='/image/backmenu' /></p>"."<br />";
            echo "No results has been found";
            }
            else {
            echo  "<center><b>". $found."<br />"."results has been found</b></center>"."<br />"."<br />"."<br />";
            }
            while ($runrows = mysql_fetch_array($results)){
                $title = $runrows['title'];
                $image = $runrows['image'];
                $category = $runrows['category'];
                $description = $runrows['movieDesc'];

                $str = "<table align='center'  cellspacing='3'  cellpadding='20'>
                <tr>
                    <th><font face='Arial, Helvetica, sans-serif'>Poster     </font></th>
                    <th><font face='Arial, Helvetica, sans-serif'>Title      </font></th>
                    <th><font face='Arial, Helvetica, sans-serif'>Category   </font></th>
                    <th><font face='Arial, Helvetica, sans-serif'>Movie Description    </font></th>

                </tr>
                <br /><br /><br />
                <tr>

                >
                     <td><img src =\" " . $runrows['image']."\"></td>
                    <td><font face='Arial, Helvetica, sans-serif'>$title</font></td>
                    <td><font face='Arial, Helvetica, sans-serif'>$category</font></td>
                    <td><font face='Arial, Helvetica, sans-serif'>$description</font></td>

                </tr>

                <br /><br /><br />

                       </table>" ;
                       echo $str."<br />";
            }
        }

    }
?>
</body>
</html>
<?php
include "footer.php";
?>
```

D. Structure and Components



E. Classes

```
<?php

class ShoppingCart

{

    protected $items = array();

    public function AddItem($product_id)

    {

        if (array_key_exists($product_id , $this->items))

            $this->items[$product_id] = $this->items[$product_id] + 1;

        else

            $this->items[$product_id] = 1;

    }

    public function EmptyCart()

    {

        $this->items = array();

    }

    public function GetItems()

    {

        return array_keys($this->items);

    }

    public function GetItemQuantity($product_id)

    {

        return $this->items[$product_id];

    }
```

```
public function GetItemCost($product_id)
{
    $cost_string = get_item_cost($product_id);
    $cost_float = "$cost_string" + 0;
    return $cost_float * intval($this->items[$product_id]);
}
public function GetShippingCost()
{
       $total = 0;
   foreach ($this->items as $product_id => $quantity )
       $total = $total + $this->GetItemShippingCost($product_id);
   return $total;
}
public function GetItemShippingCost($product_id)
{
   return $this->items[$product_id] * $this->getShippingCostFor(get_item_cost($product_id));
}
public function GetSubTotal()
{
   $total = 0;
   foreach ($this->items as $product_id => $quantity)
     $total = $total + $this->GetItemCost($product_id);
   return $total;
}
public function GetTotal()
{
```

```
        // add tax here..
        return $this->GetSubTotal() + $this->GetShippingCost();
    }
    private function getShippingCostFor($total)
    {
        if ($total < 10)
            return 4.99;
        elseif ($total < 50)
            return 10.99;
        elseif($total < 100)
            return 20.00;
        else
            return 32.50;
    }
}
?>
```