Czech University of Life Sciences in Prague

Faculty of Economics and Management

Department of Economics

Diploma Thesis

E-commerce and E-business

Author: Wasel Al-Quran

Supervisor: Ing. Mansoor Maitah Ph.D. et Ph.D.

Declaration

I declare that I have worked on my diploma thesis titled “E-commerce and E-business” by myself and I have used only the sources mentioned at the end of the thesis.

In Prague on ……

Signature

Acknowledgement

I would like to thank Ing. Mansoor Maitah PhD et PhD for his useful advice and support during my work on this Thesis

E-commerce a E-business

E-commerce and E-business

Abstract

Electronic commerce is very popular nowadays. However, security is one of the barriers, which affects the development of E-commerce. The problem needs to be addressed for the customers by the merchants. The data confidentiality and sense of security should be there for the merchant to attract more visitors to the website and sell his products online. This thesis discusses various common attack methods, and presents the defense methods according to those attacks. Because attacks may take place on the customers and the seller's site, the method of defense has been discussed from these two sides. Furthermore, this thesis has provided the basic plan for implementing security measures to E-commerce application, which includes E-commerce security policies design and disaster recovery plan.

Keywords: E-Commerce, E-Business, E-Security, Web Attacks, Web Defense, nopCommerce, ASP.NET

Abstrakt

Elektronický obchod je v dnešní době velmi populární. Nicméně, bezpečnost je jednou z překážek, která ovlivňuje jeho rozvoj. Problém je třeba řešit jak kvůli zákazníkům, tak i kvůli obchodníkům. Datová důvěrnost a pocit bezpečí by měly sloužit obchodníkovi k tomu, aby přilákal více návštěvníků na své stránky a prodal své produkty online. Tato práce se zabývá různými běžnými metodami útoků, a představuje obranné metody vůči nim. Vzhledem k tomu, že útoky mohou probíhat jak na straně zákazníka, tak i na straně prodejce, tak tato práce pojednává o útocích z obou těchto stran. Tato práce dále poskytuje základní plán pro implementování bezpečnostních opatření aplikacím E-comerce, které zahrnují bezpečnostní politiku a plán obnovy po havárii.

Klíčová slova: E-Commerce, E-Business, E-Security, Web Attacks, Web Defense, nopCommerce, ASP.NET

List of figures

Table of Contents

1. Introduction

Since the inception of the personal computers in late 80's the world has advanced to become more dependent on technologies and ICT. It's really good thing that the day to day life has become easier with the use of technology but as they say "nothing is perfect in this world only we can long towards the perfection", technologies also have vulnerabilities. These days everything is moving quickly towards cloud computing and wireless technologies, these technologies bring tremendous advantages to the consumers but not without the risks. The biggest concern is when the users or the costumers are trying to use the technologies for online transactions, Data transfers, Personal information, and financial data. The good impersonators or the con programmers will always try to get the information's from the source and it's really important to make the source secure.

The more dependent we are on the modern web technologies the more we become prone to its pros and cons. The technologies such as internet, mobile web, online banking, credit cards, and smart cards all have the possibilities of getting hacked at some point in time. E-Security refers to the protection of data, network, programs and other elements of web technologies.

In modern times the system and web applications are becoming more and more user oriented one whole program will try to cater the needs for the hoards of the user requirements just to make the application more mass friendly and famous, but this is also where the attackers get their opportunities, the bigger the program will be, the more loop holes it is likely to have for the intruders to exploit.

The key members of the electronic business are the customers, the merchant or the administrator who is operating the system (business), the third party program or, we may say, the developer of the technologies being used in the system and the last but not the least are the attackers, who tries to break into the system to steal the information.

There is an old Chinese saying that you will never be defeated if you know everything about your opponents, so thinking as an attacker is one way to protect the Cloud. This document will explain how malicious hackers attack an E-commerce system, how should administrators

protect an E-environment by using different methods, and what precautions should be taken to prevent an attack.

1.1. Study background

E Security is the integral part of the ecommerce, technology such as ASP.NET, Java, X Code, and PHP. All these technologies are constantly updating and innovating to include new application capabilities and component to their software development kit. With every new innovation comes the new threat for security. And at the same time technologies become old so fast that the support to the old one becomes rare from the provider. So it's really important for the companies to take into consideration all these factors before they were to implement new technology to the real projects.

1.2. Study area

In this thesis the close scrutiny has been done in the .NET environment using nopCommerce open source e-shop solution. The PillowHeaven Company is implementing e-shop solution for the clients to make the purchase online. The e-shop is based on nopCommerce and the research is done on the vulnerabilities of this technology and the possible suggestion for the security lapse.

1.3. Goal and Methodology

The goal of this thesis is to discuss the limitations on the modern technologies in terms of security and to be focused and precise on the research; nopCommerce technology implemented by The PillowHeaven Company has been taken into consideration for its pros and cons.

For the methodology there are factors such as Analysis of the current situation, implementation of the security methods, analysis after implementation and evaluation that's need to be taken into consideration.

2. Literature Overview

2.1. E-Commerce

2.1.1. Definition of E-Commerce

Definition of E-Commerce has not been standardized, different people define the concept with different perspective and generally it can be described as business activity through Internet.

Wikipedia says that “Electronic commerce, commonly known as e-comm, e-commerce or eCommerce, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks”

In practice, this term and a newer term, e-business, are often used interchangeably. For online retail selling, the term e-tailing is sometimes used. (VAN KETEL et. al., 2000)

According to Rosen (2002) Electronic commerce or e-commerce, covers the range of online business activities for products and services, both business-to-business and business-to-consumer, through the Internet. This section breaks e-commerce into:

- *Online shopping*. The scope of information and activities that provides the customer with the information she needs to conduct business with you and to make an informed buying decision.
- *Online Purchasing*. The technology infrastructure for the exchange of data and the purchase of a product over the Internet.

2.1.2. E-Commerce Security

Security plays a significant role in the business field, so it is necessary to understand how to keep a safe E-commerce environment. Firstly, let us take a look at different members of an E-commerce network. Actually, we may divide those members to four major parties or actors. The first one is shoppers who visit a web site and choose the product or service they want to order, and making a purchase. The second one is a merchant who is running his/her business on servers. There are many kinds of software that need to be installed on the server, and most of software is bought from the third party, which is the last legal player in an E-commerce

network. The fourth party is attackers who are the dangerous to the whole E-commerce network. Based on the above introduction of the parties involved, it is easy to see that malicious hackers threaten the whole network.

There are a lot of definitions for E-Commerce security by researchers.

Electronic commerce is buying and selling of goods and services across the internet. Commercial activities over the internet have been growing in an exponential manner over the last few years. When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an E-commerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities (OLKOWSKI, 2001).

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the “commerce chain”, the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers–including any hardware attached to the servers. (WU, 2010)

2.2. Attack Methods

Figure 2-1 clearly displays the main target points in an E-commerce network. In this section, we will discuss the basic attack methods malicious hackers may use. Those attack methods will provide the essential security knowledge to both merchants and shoppers.

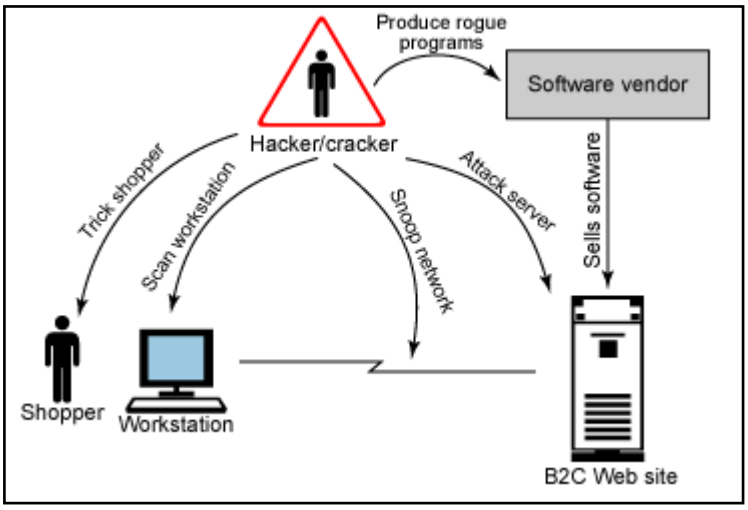

Figure 2-1 Attacker may target (adapted from IBM)

2.2.1. Tricking the shoppers

One of the most easiest and most often happened attack method. Hackers will gain your trust in some way to take sensitive information and use it for malicious purpose. Many researchers defined tricking shoppers

Tricking shoppers is the easiest and most profitable attack method in E-commerce. Basically, attackers trick shoppers to acquire their personal information, such as password, the challenge question's answer, bank account and so on. The most common method used by attackers is the social engineering attack. [WU, 2010]

Social engineering is the way hackers use to get information directly from people. For this reason it is also referred as human hacking

In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural

helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques. (techtarget.com)

Another common form of social engineering attacks are phishing schemes. Typo pirates play on the names of famous sites to collect authentication and registration information. In this case the hackers will register a site name closer to known web sites for example ameyzon.com instead of amazon.com and they will send e mail pretending to be from amazon.com and asking to fill registration information following a link inside the e mail which leads to the fraud website.

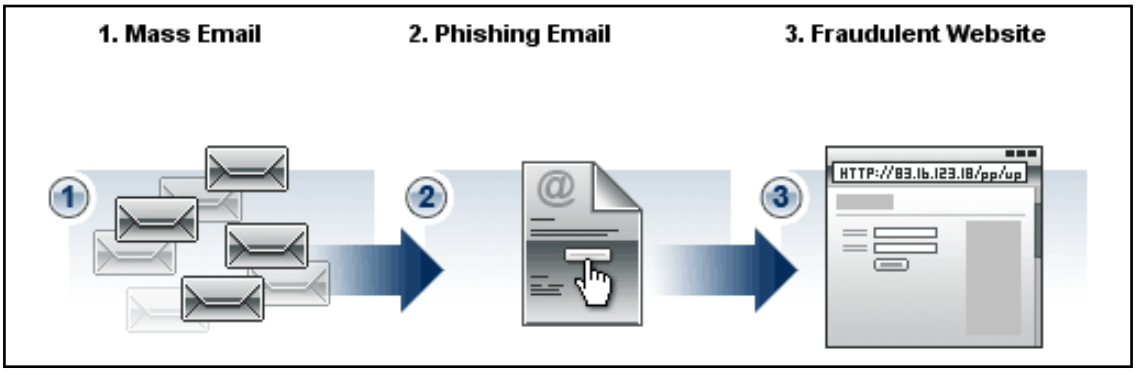

Figure 2-2 How email phishing works (adapted from toontowncentral.com)

2.2.2. Sniffing the network

While a shopper is communicating with the e-commerce server the attacker will be in between controlling the data transaction and collects shopper information.

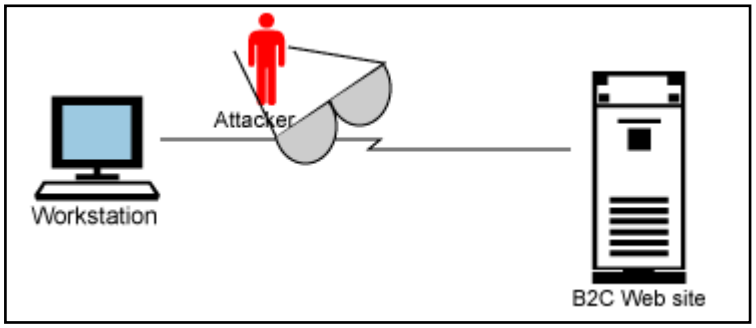

Figure 2-3 Attacker sniffing the network between client and server (adapted from IBM)

There are points in the network where this attack is more practical than others. If the attacker sits in the middle of the network, then within the scope of the Internet, this attack becomes

impractical. A request from the client to the server computer is broken up into small pieces known as packets as it leaves the client's computer and is reconstructed at the server. The packets of requests are sent through different routes. The attacker cannot access all the packets of a request and cannot decipher what message was sent. (IBM)

2.2.3. Guessing the passwords

This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper. For example, if the shopper uses their child's name as the password. Automated attacks have a higher likelihood of success, because the probability of guessing a user ID/password becomes more significant as the number of tries increases. Tools exist that use all the words in the dictionary to test user ID/password combinations, or that attack popular user ID/password combinations. The attacker can automate to go against multiple sites at one time. (IBM)

2.2.4. Using denial of service attacks

In which an attacker uses specialized software to send a flood of data packets to the target computer with the aim of overloading its resources to make the computer to deny access for the intended user

Definition of Denial of service:

- Is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all. (Wikipedia)
- Denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target. (techterget.com)

There are different ways of DoS including TCP floods, a stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used,

ICMP echo request/reply (e.g., ping floods), a stream of ICMP packets are sent to a victim IP address, and UDP floods, stream of UDP packets are sent to the victim IP address.

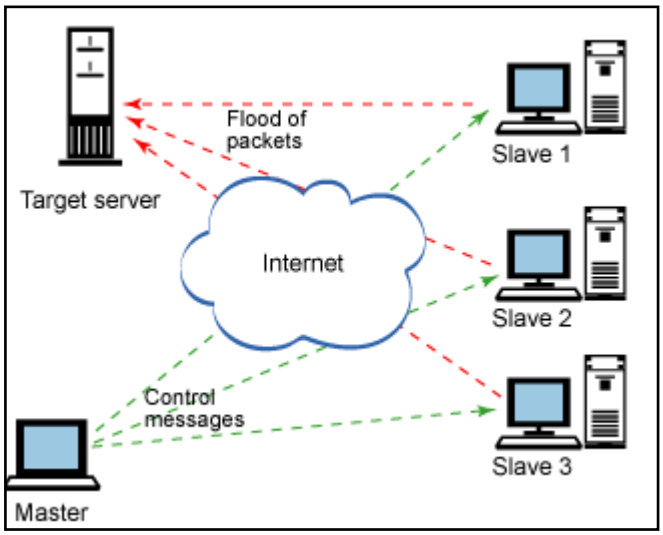

Figure 2-4 denial of service attack (adapted from IBM)

2.2.5. Using known server bugs

The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task.

2.2.6. Using server root exploits

Root exploits refer to techniques that gain super user access to the server. This is the most coveted type of exploit because the possibilities are limitless. When you attack a shopper or his computer, you can only affect one individual. With a root exploit, you gain control of the merchants and all the shoppers' information on the site. There are two main types of root exploits: buffer overflow attacks and executing scripts against a server. (IBM)

2.2.7. Buffer overflow

If an attacker has gained access into the root of site, it means all of the E-Commerce users' information is gained. The buffer overflow is the most common method used by the attackers to access the servers' kernel.

Buffer overflow: Over 70% of vulnerabilities that have been recorded have a buffer overflow in the exploit somewhere (Conway, 2004). Let us see how this buffer overflow works. Actually, a buffer is the place which temporarily stores data, and each buffer has a limited space. When attackers set overwritten data into a buffer which does not have sufficient space to keep the data, the extra data will overflow into an adjacent buffer, which may contain other data. In this case, those data stored in the adjacent buffer will be replaced by overwritten data. Once the system invokes the data, which are stored in the adjacent buffer, those overwritten data will be executed. Normally, attackers will design those overwritten data in order to gain access into the root of system after system has been running overwritten data.

2.3. Defense

This section will demonstrate how to keep a secure E-commerce environment. The security work does not only belong to merchants but also to shoppers. The cooperation of merchants and shoppers should be seamless, so that attackers may not easily find the bugs to attack. According to the mentioned attack methods, this chapter will discuss how to protect an Ecommerce network work properly. Figure 2-5 shows the basic defense methods.

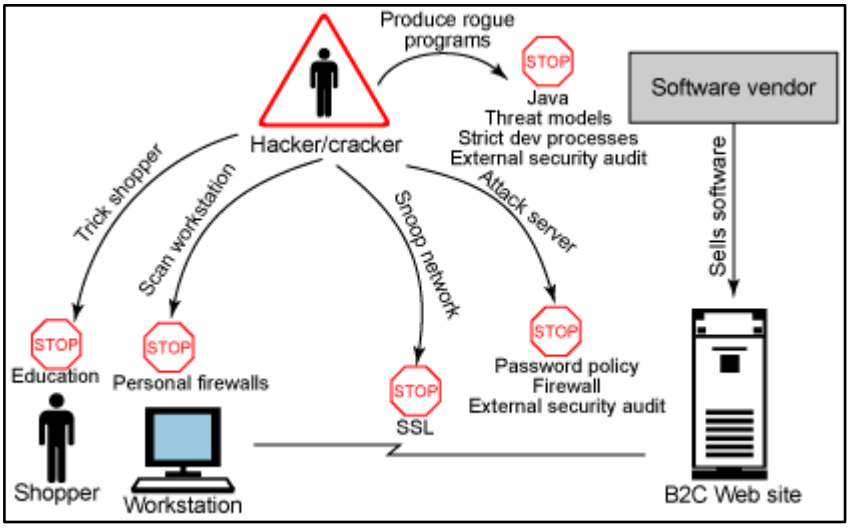

Figure 2-5 Attacks and their defenses (adapted from IBM)

At the end of the day, your system is only as secure as the people who use it. Education is the best way to ensure that your customers take appropriate precautions:

- Install personal firewalls for the client machines.
- Store confidential information in encrypted form.
- Encrypt the stream using the Secure Socket Layer (SSL) protocol to protect information flowing between the client and the e-Commerce Web site.
- Use appropriate password policies, firewalls, and routine external security audits.
- Use threat model analysis, strict development policies, and external security audits to protect ISV software running the Web site.

2.3.1. Education

Your system is only as secure as the people who use it. If a shopper chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system. In this case, there is likely physical security involved because the administrator client may not be exposed outside the firewall. Users need to use good judgment when giving out information, and be educated about possible phishing schemes and other social engineering attacks.

2.3.2. Setting a safe password

The most users select their password from their familiar things such as birth day, children's name, or pet's name. However, an attacker could pick up personal information such as children's name, spouse's name, birthday and even more. It is important that shoppers choose a strong password to login their account. What makes a strong password? Length is one of factor, and containing a variety of character is the other factor. When a shopper registers an account from a web site, it is a good idea to ask the shopper to have a password of a minimum length, and use a variety of characters. If shoppers cannot come up with a good password, merchants may guide shoppers using a safe password generator which we can find from many web sites.

2.3.3. Managing Cookies

When shoppers open an account in a web shop, they may use a cookie to store their passwords, Email addresses, account numbers and so on, so shoppers do not need to enter this information again when they login to the web site again. Basically, websites also use cookies

to manage shopping carts and authenticate users (Schrenk, Michael, 2007). The feature of cookies provides convenient service to shoppers, but it also provides a chance for an attacker to steal information. Once shoppers apply cookies, the certain information shoppers enter into the web site will be recorded into the shoppers' hard disk. Once attackers access the shoppers' computer, they may scan the cookies' file and find the shoppers' personal information. How can the shoppers avoid this issue? The easiest way is to stop using cookies, and most users can reconfigure their browsers to turn off cookies.

2.3.4. Personal Firewall

Installing a personal firewall is one way to protect the shoppers' work station. A personal firewall is an application which controls network traffic to and from a computer. While it is different from a conventional firewall, a personal firewall only works on the computer which has a firewall application installed. After a personal firewall has been installed, it will control the incoming and outgoing traffic according to the security policies. Furthermore, a personal firewall provides an intrusion detection system which is designed to detect unwanted attempts at accessing, manipulating, and/or disabling computer systems.

A personal firewall has some basic features which might help shoppers:

- Shoppers can decide which programs can and cannot access the local network.
- It can hide the shoppers' computers from port scans by not responding to unsolicited network traffic.
- It can monitor if there are any applications sniffing the shoppers' data.
- It can protect against Trojan accessing the shoppers' computers from the Internet.
- It can provide information of a destination server which is communicating with the shoppers' work stations.
- It can scan the shoppers' computers when the shoppers turn on computers to avoid malicious and other unwanted programs.

It is necessary to install a firewall for shoppers, and the shoppers have to update their firewall frequently. Because bugs may exist in the application firewall as well, installing new patches will decrease attacks.

2.3.5. Digital signatures

A digital signature is similar to a personal signature and it verifies two important things pieces of information in electronic communication. First, it checks whether the message comes from an original sender. Second, it verifies if the message has been changed after it was sent. How does a digital signature work in an E-commerce system? Firstly, a web site will use a one-way hashing algorithm to create a fixed length message digest from the data, which is going to be sent. After that, the message digest will be encrypted by the web site's private key in order to get digital signature. Figure 2-6 shows the steps to create a digital signature.

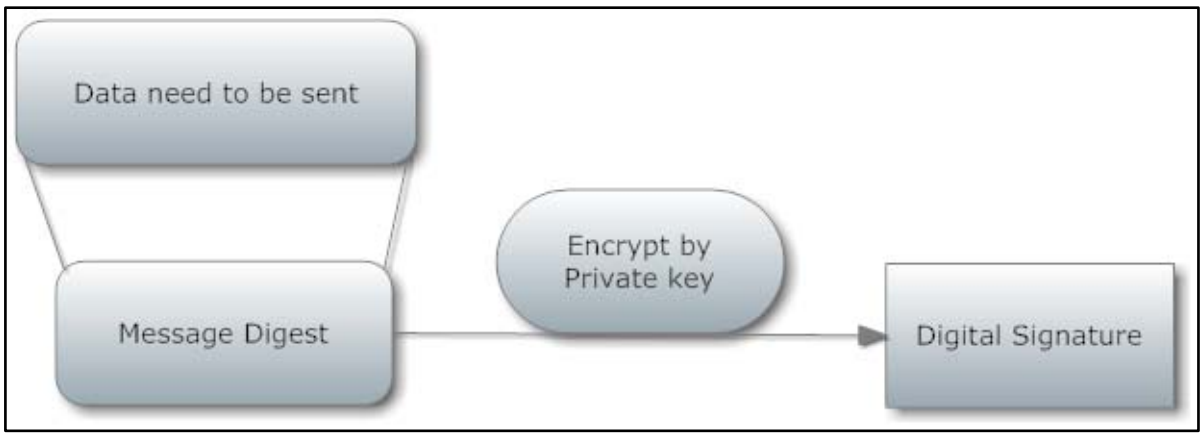

Figure 2-6 Steps to create a digital signature (own drawing)

The created digital signature will be sent together with the data, which has to be sent to the shoppers. When the shoppers receive the digital signature and the data, they will decrypt the digital signature with a public key to obtain the first message digest, which we call digest1 here. At same time, the shoppers calculate the second message digest (called digest2) by using same method as the web site, so the second message digest is calculated from the received data. By comparing digest1 and digest2, the shoppers will know if this Data need to be sent Message Digest Encrypt by Private key Digital Signature message has been changed or not. If digest1 is the same as digest2, the shoppers will accept the digital signature as a legal one. The shoppers will discard the distorted message when the digest1 is different from digest2. Figure 2-7 illustrates the whole process of digital signature verification.

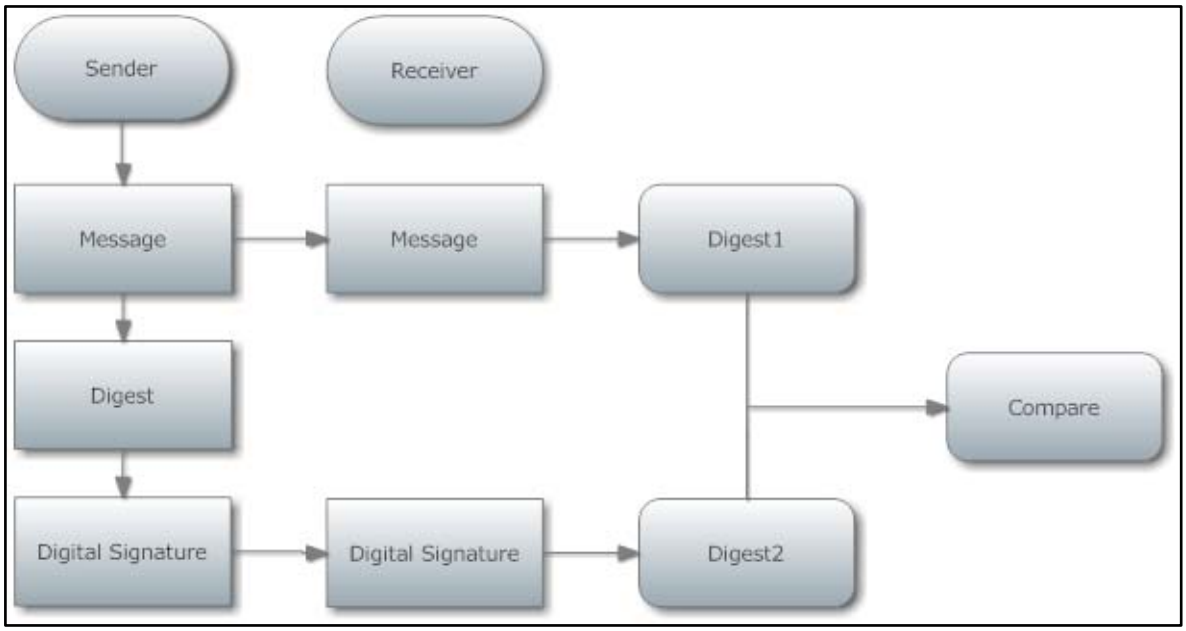

Figure 2-7 Authentication of the message using a digital signature (own drawing)

2.3.6. Server Firewall

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines.

A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is a resource (for example, a fake payment server) placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall. These servers are closely monitored, and any access by an attacker is detected.

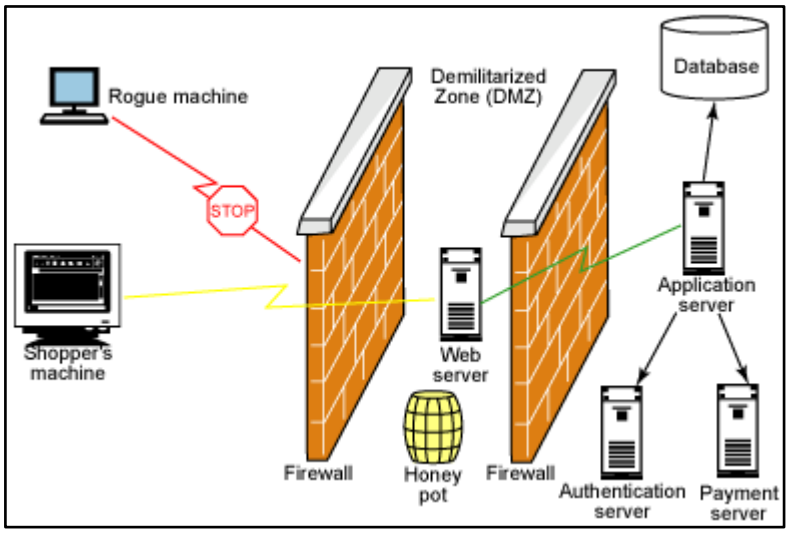

Figure 2-8 Firewalls and honey pots (adapted from IBM)

2.3.7. SSL and TLS

Transport Layer Security (TLS) and its predecessor SSL are security protocols that encrypt data transferring between the shoppers' workstation and the sites' servers and prevent third party listening and tampering.

Secure Sockets Layer is a protocol designed to work, as the name implies, at the socket layer, to protect any higher-level protocol built on sockets, such as telnet, ftp, or HTTP (Milutinovic, Veljko, 2002). A good example of applying SSL is HTTPS. Https:// indicates that users are connecting to a secure web server. For instance, when customers go to the CSOB e-banking site to login to their bank account, they will see a secure web site connection address: https://bb24.csob.cz/.

How does SSL/TLS work? The SSL/TLS client and server communicate by a handshaking procedure. Figure 2-9 illustrates the steps through which SSL/TLS achieves a secure conversation.

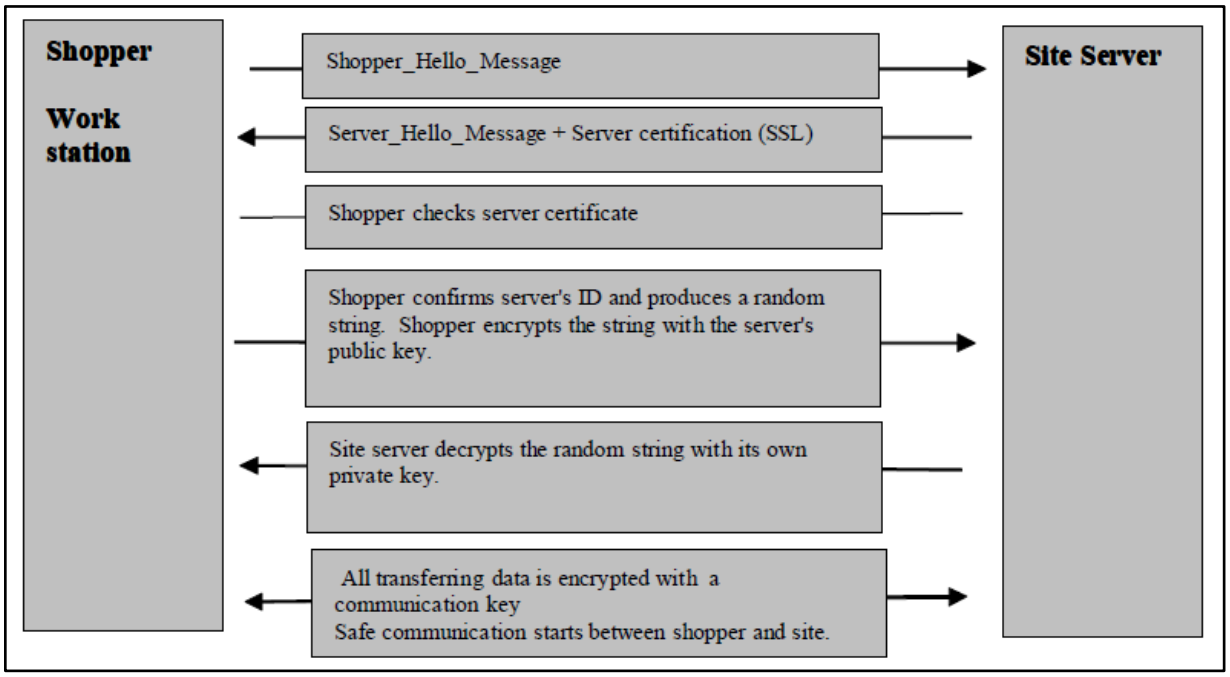

Figure 2-9 SSL conversation steps (Adapted from IMB)

Firstly, a shopper sends a "Hello" message to start conversation, and this message includes the list of cryptology algorithms which shoppers are supported. The site receives the message and replies with a server_hello message. The server_hello message contains the suitable algorithm chosen from the list and its site's digital certificate. In the same way as we mentioned in the digital certificate section, the shopper verifies the digital signature to make sure if this certificate can be trusted. After the site of identification has been confirmed, the shopper site will generate a random string and encrypt it with the public key received from the site. The encrypted random string is sent to the site and it will be decrypted by the site's private key. In this way, no one can sniff and tamper this random string. The algorithm of the symmetric-key will be used after both sides have the same random string. The random string will be taken as the key to encrypt and decrypt the later message, which will be transferred between the shoppers and the web site. In brief, SSL and TLS apply both a symmetric-key algorithm and an asymmetric-key algorithm to ensure the security of the transmission.

If the site is not recognized by a trusted certificate authority, then the browser issues a warning as shown in Figure 2-10.

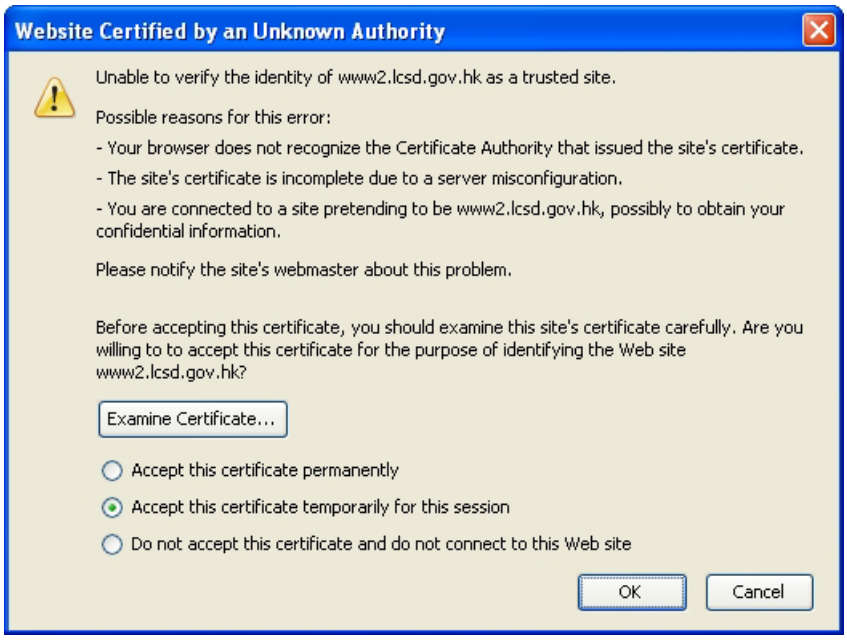

Figure 2-10 Warning to user (result from Mozilla Firefox)

2.3.8. Updating patches

As it was mentioned in the beginning of this section, patches may display the bugs existing in the system or software to the attackers. Updating patches can perfect the system and software, so that both the E-commerce network administrators and the shoppers should constantly install the latest version of patches for keeping a secure E-shopping environment.

2.3.9. Monitoring logs

Finding the weak points of an E-commerce system is also one of the defense strategies. Monitoring and analyzing security logs may achieve this defense goal. For instance, if there is anyone falling into a honey pot, the honey pot will record a security log to network administrators. It would be good that network administrators read those logs frequently and understand which points are the targets of the intruders, so that the administrators can update the system according to the bugs displayed on the log. Monitoring the entire Ecommerce network will help administrators to react quickly when attacks start. For instance, administrators may monitor the network through Intrusion Detection System (IDS).

3. Improving of E-Commerce security for PillowHeaven

PillowHeaven is an existing company which implements E-Commerce application for selling products online. PillowHeaven offers wide range of decorative pillows, quilts, blankets and bags under Dutch Decor brand in the Czech Republic market and it was founded in February 2010.

PillowHeaven for the period of its existence has built strong market position in the interior textiles and nowadays it needs more security implementations.

In this part of thesis I want to analyze how are PillowHeaven secured and which type of attack methods can be dangerous and which kind of defense methods must be implemented.

3.1. Requirements

PillowHeaven E-Commerce application was built on .NET environment and the following hardware and software required for making any implementation on it:

1. Hardware requirements
    - PC that has a 1.6GHz or faster processor
    - 1 GB (32 Bit) or 2 GB (64 Bit) RAM
    - 3GB of available hard disk space after OS installed
    - 5400 RPM hard disk drive
    - DirectX 9 capable video card running at 1024x768 or higher-resolution display
2. Software requirements
    - Supported operation systems
        - Windows 7
        - Windows Vista
        - Windows XP
        - Windows Server 2003
        - Windows Server 2008
    - Supported Web Servers

- Internet Information Service (IIS) 5.1 or above
- ASP.NET 4.0

- Supported Databases
  - MSSQL 2005 or above
- Supported browsers
  - Microsoft Internet Explorer 6 and above
  - Mozilla Firefox 2.0 and above
  - Google Chrome 1.x
  - Apple Safari 2.x
  - Visual Studio 2010 or above

3.2. Methodology

Implementing security methods for PillowHeaven is illustrated in Figure 3-1. The implementation roadmap consists of 4 stages which are the analysis current situation, implementation security methods, analysis after implementation and evaluation.

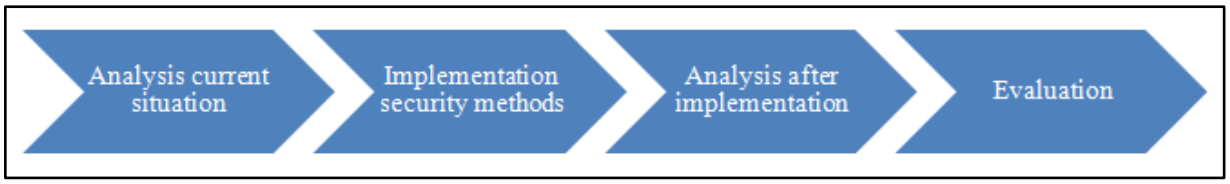

Figure 3-1 Security implementation roadmap (own drawing)

Based on the roadmap in Figure 3-1, security methods are implemented to PillowHeaven.

1. **Analysis current situation**

   In this step researcher will analyze current satiation of PillowHeaven. How customers are protected. Find out implemented security methods and application vulnerability.
2. **Implementation security methods**

   In this step researcher will implement security methods and improve existing methods which were found on first step.
3. **Analysis after implementation**

In this step researcher will analyze situation after implementation and improvement security methods to PillowHeaven.

4. **Evaluation**

   At the end of all processes researcher will analyze how implementation security methods affected and makes comparison before and after implementation.

3.3. Implementation of security methods

According to above chapter methodology researcher will implement necessary secure methods and improve existing methods.

Researcher will be focused on application architecture rather than customer side.

3.3.1. Current system analysis

PillowHeaven built on .NET environment and nopCommerce solution.

NopCommerce is a fully customizable shopping cart. It's stable and highly usable. NopCommerce is an open source e-commerce solution that is ASP.NET 4.0 based with a MS SQL 2005 (or higher) backend database. Easy-to-use shopping cart solution is uniquely suited for merchants that have outgrown existing systems, and may be hosted with merchant's current web host or nopCommerce hosting partners. It has everything to get started in selling physical and digital goods over the internet.

Analyze for security on PillowHeaven e-commerce application gives following results:

1. **Configuration files**

   The Web.config is an XML based configuration file for the entire application and resides in the application root. It provides the application wide settings for the entire application. And PillowHeaven has following mistakes on configuration file:

   - **Custom errors disabled**

     When custom errors disabled as shown below, ASP.NET provides detailed error message to clients by default

     Vulnerable configuration on PillowHeaven:

     ```
     <customErrors mode="Off"></customErrors>
     ```

In itself, knowing the source of an error may not seem like a risk to application security, but consider this: the more information a hacker can gather about a Web site, the more likely it is that he will be able to successfully attack it. An error message can be a gold mine of information to an attacker. A default ASP.NET error message lists the specific versions of ASP.NET and the .NET framework which are being used by the Web server, as well as the type of exception that was thrown. Just knowing which Web-based applications are used (in this case ASP.NET) compromises application security by telling the attacker that the server is running a relatively recent version of Microsoft Windows and that Microsoft Internet Information Server (IIS) 6.0 or later is being used as the Web server. The type of exception thrown may also help the attacker to profile Web-based applications; for example, if a SqlException is thrown, then the attacker knows that the application is using some version of Microsoft SQL Server.

- **Debugging enabled**

  Deploying Web-based applications in debug mode is a very common mistake. Virtually all Web-based applications require some debugging. Visual Studio 2005 will even automatically modify the Web.config file to allow debugging when you start to debug your application. And, since deploying ASP.NET applications is as simple as copying the files from the development folder into the deployment folder, it's easy to see how development configuration settings can accidentally make it into production, compromising application security.

  Vulnerable configuration on PillowHeaven:

  ```
  <compilation debug="true" targetFramework="4.0">
  ```

- **Sliding Expiration used**

  All authenticated ASP.NET sessions have a timeout interval to protect the application security. The default timeout value is 30 minutes. So, 30 minutes after user first logs into any of these Web-based applications, he will automatically be logged out and forced to re-authenticate his credentials.

  Vulnerable configuration on PillowHeaven:

<forms slidingExpiration="true">

- **Cookies Accessible through Client-Side Script**

  In Internet Explorer 6.0, Microsoft introduced a new cookie property called Http Only. While you can set the property programmatically on a per-cookie basis, you also can set it globally in the site configuration.

  Vulnerable configuration on PillowHeaven:

  <httpCookies httpOnlyCookies="false">

2. **SQL Injection**

   SQL Injection occurs when someone enters a part of a SQL Command as part of user input, querystring, or cookie. For example, if person enters " or '1' = '1' in a password textbox, that might be interpreted as part of the SQL command and cause the password to always be accepted.

   During analysis PillowHeaven for SQL injection, there were no serious bugs found. But, it is recommended to consider security methods against SQL injection for future application changes. These methods will be given in implementing section below.

3. **JavaScript Injection**

   If someone enters javascript in a textbox they can possibly attach an event to a submit button that will execute whenever anyone presses submit. The event can be used to send private information to the attacker.

   In PillowHeaven security methods against javascript injection were used. And it is almost automatically prevented by the Request Validation feature of ASP.NET, which is always set to being on by default.

4. **Secure Sockets Layer**

   SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

To be able to create an SSL connection a web server requires an SSL Certificate. And current situation of PillowHeaven requires SSL certificate. And installation steps will be described in the implementation sections of this thesis.

5. **Using CAPTCHA for forms**

   CAPTCHA stands for "completely automated public Turing test to tell computers and humans apart." What it means is, a program that can tell humans from machines using some type of generated test. A test most people can easily pass but a computer program cannot.

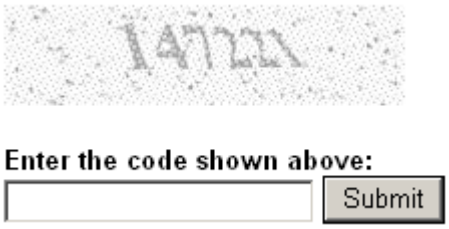

Figure 3-2 CAPTCHA (adapted from reCAPTCHA)

You've probably encountered such tests when signing up for an online email or forum account. The form might include an image of distorted text, like that seen above Figure 3-2, which you are required to type into a text field.

The idea is to prevent spammers from using web bots to automatically post form data in order to create email accounts (for sending spam) or to submit feedback comments or guestbook entries containing spam messages. The text in the image is usually distorted to prevent the use of OCR (optical character reader) software to defeat the process. Hotmail, PayPal, Yahoo and a number of blog sites have employed this technique.

PillowHeaven doesn’t have CAPTCHA for its HTML forms. So, it’s required to develop CAPTCHA project and apply to all forms especially for registration and newsletter submit form.

3.3.2. Implementing security methods

According to chapter above researcher will implement security methods where PillowHeaven has vulnerability and provide with guidelines

1. **Modifying Configuration files**

   - **Modify custom errors**

     Secure configuration:

     ```
     <customErrors mode="RemoteOnly"></customErrors>
     ```

     Application security can be built up to prevent such information leakage by modifying the mode attribute of the <customErrors> element to On or RemoteOnly. This setting instructs Web-based applications to display a nondescript, generic error message when an unhandled exception is generated. Another way to circumvent this application security issue is to redirect the user to a new page when errors occur by setting the defaultRedirect attribute of the <customErrors> element. This approach can provide even better application security because the default generic error page still gives away too much information about the system (namely, that it's using a Web.config file, which reveals that the server is running ASP.NET).

   - **Modify compilation**

     Secure configuration:

     ```
     <compilation debug="false" targetFramework="4.0">
     ```

     Leaving debugging enabled is dangerous because you are providing inside information to end users who shouldn’t have access to it, and who may use it to attack your Web-based applications. For example, if you have enabled debugging and disabled custom errors in your application, then any error message displayed to an end user of your Web-based applications will include not only the server information, a detailed exception message, and a stack trace, but also the actual source code of the page where the error occurred.

   - **Modify Sliding Expiration**

     Secure configuration:

     ```
     <forms slidingExpiration="true">
     ```

     The slidingExpiration setting is an application security measure used to reduce risk to Web-based applications in case the authentication token is stolen. When set to false, the specified timeout interval becomes a fixed period of time from the initial login, rather than a period of inactivity. Attackers using a stolen

authentication token have, at maximum, only the specified length of time to impersonate the user before the session times out. Because typical attackers of these Web-based applications have only the token, and don't really know the user's credentials, they can't log back in as the legitimate user, so the stolen authentication token is now useless and the application security threat is mitigated. When sliding expiration is enabled, as long as an attacker makes at least one request to the system every 15 minutes (or half of the timeout interval), the session will remain open indefinitely. This gives attackers more opportunities to steal information and cause other mischief in Web-based applications. To avoid this application security issue altogether, you can disable sliding expiration by setting the slidingExpiration attribute of the <forms> element to false.

- **Modify Cookies Accessibility**

  Secure configuration:

  ```
  <httpCookies httpOnlyCookies="true">
  ```

  Any cookie marked with this property will be accessible only from server-side code, and not to any client-side scripting code like JavaScript or VBScript. This shielding of cookies from the client helps to protect Web-based applications from Cross-Site Scripting attacks. A hacker initiates a Cross-Site Scripting (also called CSS or XSS) attack by attempting to insert his own script code into the Web page to get around any application security in place. Any page that accepts input from a user and echoes that input back is potentially vulnerable. For example, a login page that prompts for a user name and password and then displays “Welcome back, <username>” on a successful login may be susceptible to an XSS attack.

  Message boards, forums, and wikis are also often vulnerable to application security issues. In these sites, legitimate users post their thoughts or opinions, which are then visible to all other visitors to the site. But an attacker, rather than posting about the current topic, will instead post a message such as “<script>alert(document.cookie);</script>”. The message board now includes

the attacker's script code in its page code—and the browser then interprets and executes it for future site visitors. Usually attackers use such script code to try to obtain the user's authentication token (usually stored in a cookie), which they could then use to impersonate the user. When cookies are marked with the HttpOnly property, their values are hidden from the client, so this attack will fail.

As mentioned above, it is possible to enable HttpOnly programmatically on any individual cookie by setting the HttpOnly property of the HttpCookie object to true. However, it is easier and more reliable to configure the application to automatically enable HttpOnly for all cookies. To do this, set the httpOnlyCookies attribute of the <httpCookies> element to true.

2. **Preventing SQL injection attacks**
   - **Replace SQL Commands with Parameterized queries**

     One way to prevent SQL injection 100% of the time is by replacing all SQL Commands with parameterized queries. The queries can be stored procedures, but they do not have to be. Stored procedures are a little more efficient because they optimize execution plan, but parameterized queries that are not stored procedures are also safe with regard to SQL injection. The information in the parameterized fields is always treated as a literal by SQL server and can never be executed as part of the SQL instruction itself. Using parameterized queries in all SQL Commands in an application prevents SQL injection through: 1) user input; 2) query strings; and 3) cookies. The work involved in implementing it would require that every SQL Command that uses input from user, query string, or cookie be converted to parameterized query.
   - **Replace SQL Commands with LINQ to SQL**

     LINQ to SQL, when used exclusively for data access, eliminates the possibility of SQL injection in your application for one simple reason: every SQL query that LINQ executes on your behalf is parameterized.
   - **Create "Blacklist" of special characters and words**

Here is a shortlist of five predefined entities in xml that people often try to sanitize (remove) from user input:

1	quot	“
2	amp	&
3	apos	‘
4	Lt	<
5	Gt	>

Here is another example blacklist:

```
public static string[] blackList = {"–",";–",";","/*","*/","@@","@",
                                    "char","nchar","varchar","nvarchar",
                                    "alter","begin","cast","create","cursor",
                                    "declare","delete","drop","end","exec","execute",
                                    "fetch","insert","kill","open",
                                    "select", "sys","sysobjects","syscolumns",
                                    "table","update"};
```

Two drawbacks of SQL Injection "Blacklists" of special characters or words:

1) Blacklisted words and characters change over time. For example, => (lambda) is new C# expression that was recently introduced.

2) Frustrates users trying to enter real data. For example, a user will become frustrated if the quote mark they enter in a textbox mysteriously vanishes each time they enter it.

3. Preventing JavaScript Injection attacks

Javascript injection is automatically prevented by the Request Validation feature ASP.NET, which is always set to being on by default.

But, it is better to know standard defense methods. And in case of not using or not existing Validation Request, following methods must be applied:

- **Using parameterized queries**

  Use parameterized queries or stored procedures to access a database as opposed to using string concatenation.

- **Using html encode**

  One easy method of preventing javascript injection attacks is html encode of any data entered by website users.

  What does it mean to HTML encode a string?

  When you HTML encode a string, dangerous characters such as < and > are replaced by HTML entity references such as < and >. So when the string <script>alert("Boo!")</script> is HTML encoded, it gets converted to <script>alert("Boo!")</script>. The encoded string no longer executes as a javascript script when interpreted by a browser.

- **HTML input limitations**

  Limit the amount of characters in input fields (e.g. username and password fields) to a proper amount. And this amount must be less or equal to specific database column.

- **HTML input validation**

  Validate text input for improper characters (like ‘). For ASP.NET it can be used RequiredFieldValidator and RegularExpressionValidator.

4. **Implementation of SSL certificate**

   SSL stands for "Secure Sockets Layer". It commonly uses port 443 to connect computers to a secure server on the Internet. SSL is most often used for transmitting credit card, tax, banking, or personal information to a business server somewhere. Examples of SSL: you are purchasing a DVD from Amazon.com, you are filing your taxes online, or you are transferring funds between your checking and savings accounts.

   For implementing SSL certificate. First of all, we should buy it.

   There are a lot of SSL certificate providers in the world such as GoDaddy, Verisign, Comodo, Digicert, Thawte and also can be bought by hosting providers.

   After buying SSL certificate it should be installed as well.

   SSL certificate installation steps in Microsoft IIS 7:

   - Open the ZIP file containing SSL certificate. Save the file named domain_name.cer to the desktop of the web server.

- Click on Start, then Administrative Tools, then Internet Information Services (IIS) Manager.
- Click on the server name.
- From the center menu, double-click the "Server Certificates" button in the "Security" section (near the bottom of the menu) as shown in Figure below.

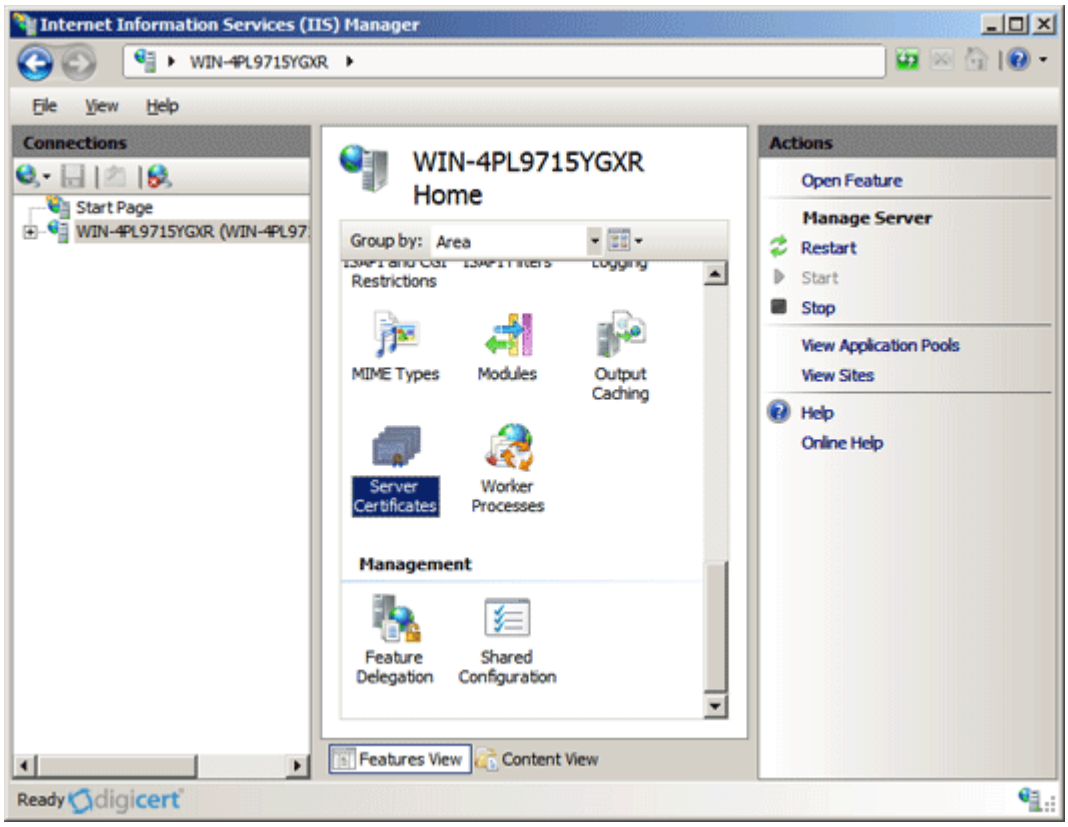

Figure 3-3 SSL installation step 1 in Microsoft IIS 7 (Adapted from Digicert)

- From the "Actions" menu (on the right), click on "Complete Certificate Request." This will open the Complete Certificate Request wizard.

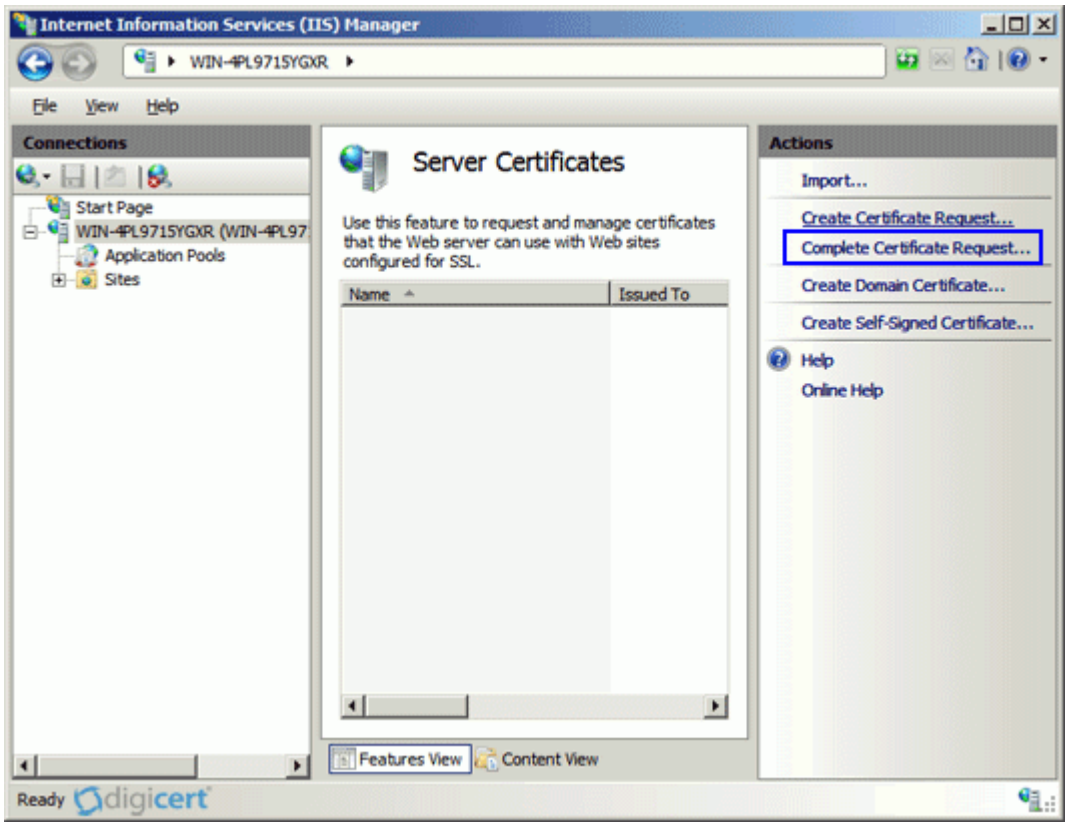

Figure 3-4 SSL installation step 2 in Microsoft IIS 7 (Adapted from Digicert)

- Browse to domain_name.cer file that was given by SSL providers. It will then require entering a friendly name. The friendly name is not part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.

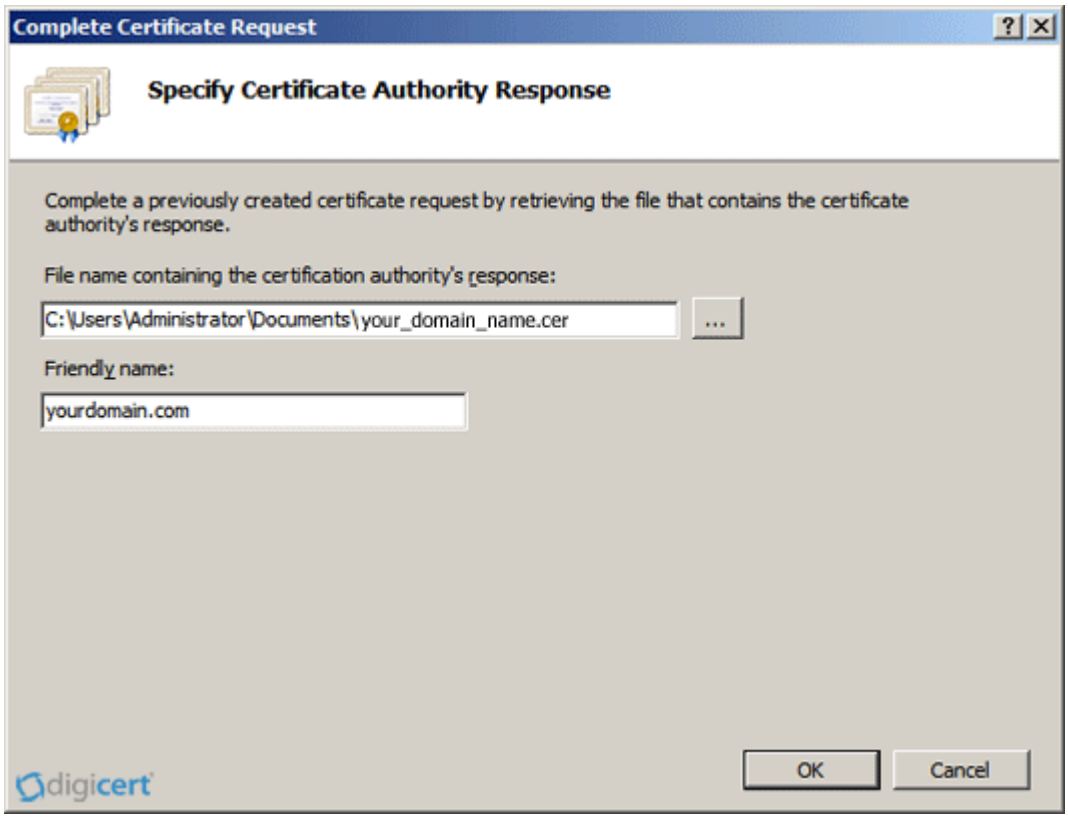

Figure 3-5 SSL installation step 3 in Microsoft IIS 7 (Adapted from Digicert)

- Clicking "OK" will install the certificate to the server.
- Once the SSL certificate has been successfully installed to the server, it needs to assign that certificate to the appropriate website using IIS.
- From the "Connections" menu in the main Internet Information Services (IIS) Manager window, select the name of the server to which the certificate was installed.
- Under "Sites," select the site to be secured with SSL.
- From the "Actions" menu (on the right), click on "Bindings." This will open the "Site Bindings" window.

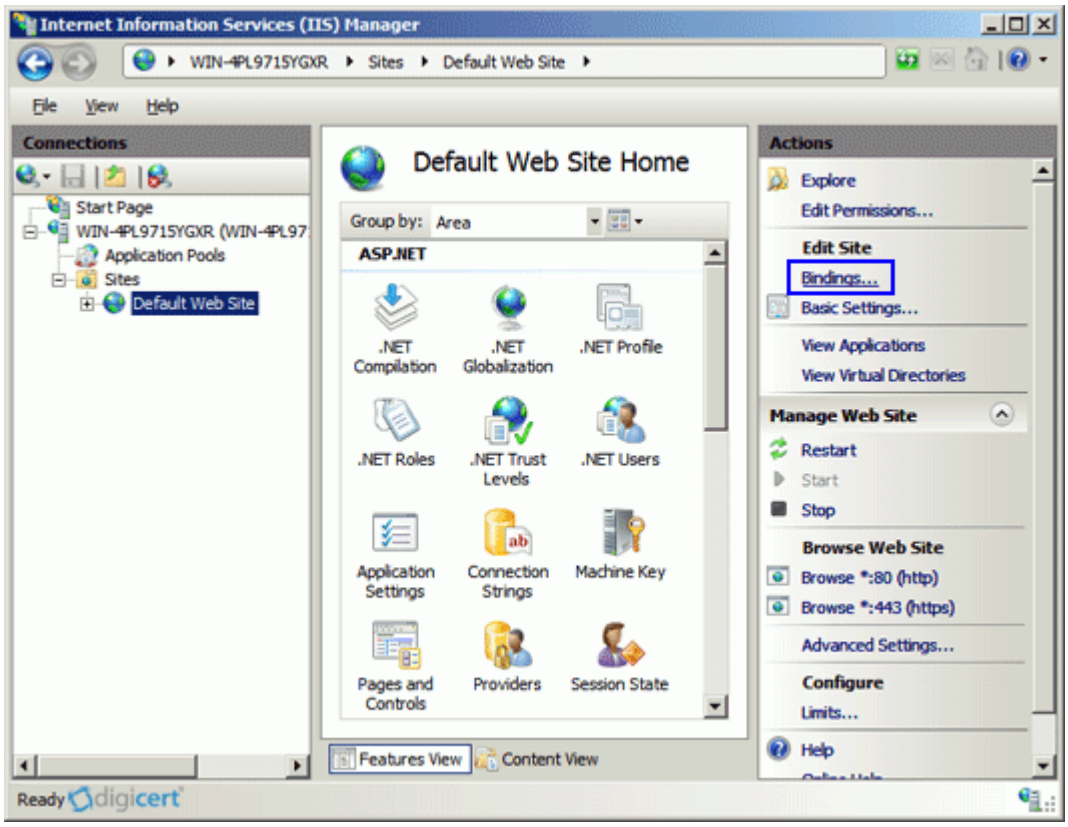

Figure 3-6 SSL installation step 4 in Microsoft IIS 7 (Adapted from Digicert)

- Under "Sites," select the site to be secured with SSL.

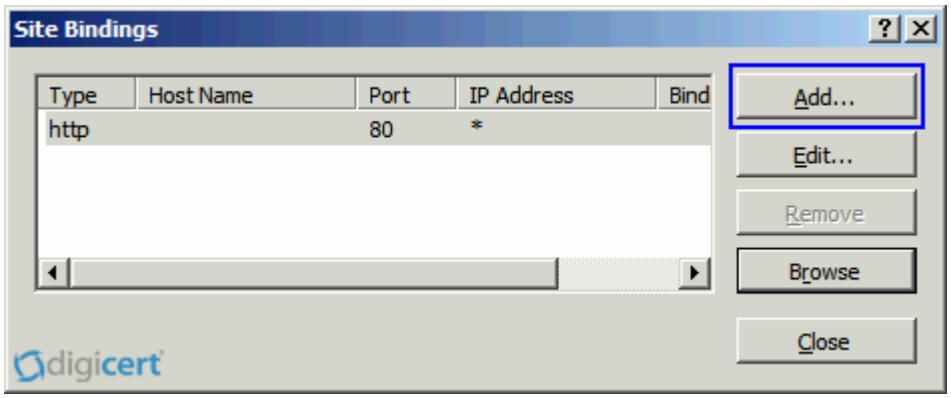

Figure 3-7 SSL installation step 5 in Microsoft IIS 7 (Adapted from Digicert)

- Under "Type" choose https. The IP address should be the IP address of the site or All Unassigned, and the port over which traffic will be secured by SSL is usually 443.

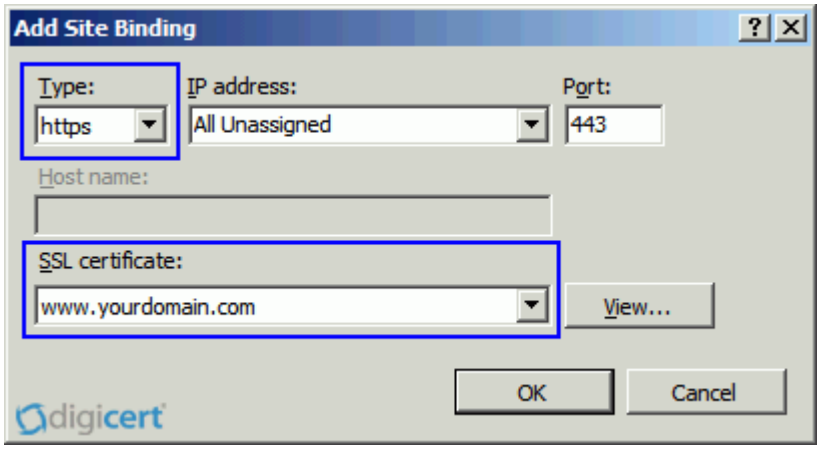

Figure 3-8 SSL installation step 6 in Microsoft IIS 7 (Adapted from Digicert)

- Click "OK."

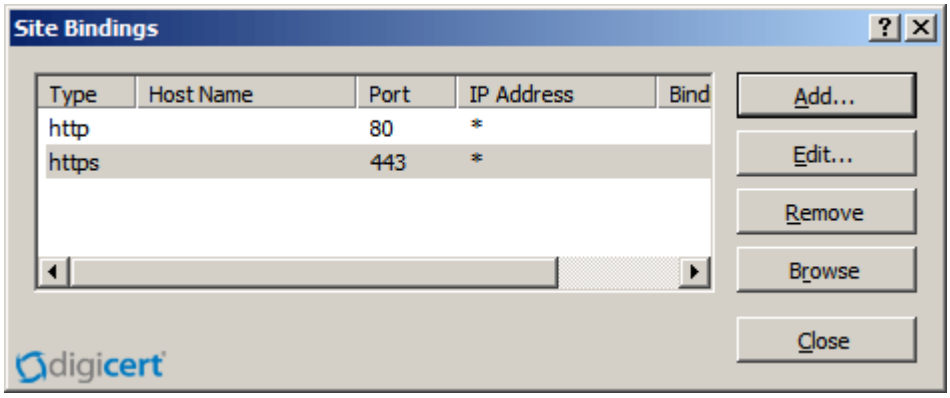

Figure 3-9 SSL installation step 7 in Microsoft IIS 7 (Adapted from Digicert)

- SSL certificate is now installed, and the website configured to accept secure connections.

After installation of SSL certificate, it needs to implement in PillowHeaven application as well. And it can be done using ASP.NET Request.IsSecureConnection method as follow:

```
if (!Request.IsSecureConnection)
{
        string redirectUrl = Request.Url.ToString().Replace("http:", "https:");
        Response.Redirect(redirectUrl);
}
```

5. Implementation CAPTCHA

Before using CAPTCHA however, developers should consider how it will affect your site's accessibility to the blind and other visually impaired visitors. For example, PayPal attempts to address this problem on their sign up form by including a link to an audio file, in which a voice spells out the image text.

There are a lot of open source CAPTCHA API's to use. And I'll choose reCAPTCHA to implement it for PillowHeaven.

Last version of reCAPTCHA is available here:

http://recaptcha.googlecode.com/files/recaptcha-dotnet-1.0.5.0-binary.zip

[Accessed on 4.3.2011]

Implementation reCAPTCHA into PillowHeaven is following:

2. Download necessary library from the link above.
3. Add a reference on PillowHeaven to library/bin/Release/Recaptcha.dll:

   It can be done on the Visual Studio Website menu, by choosing Add Reference and then clicking the .NET tab in the dialog box. And selecting the Recaptcha.dll component from the list of .NET components and then clicking OK.
4. Insert the reCAPTCHA control into the form which must be protected. Then it needs to insert following code at the top of the aspx page:

   ```
   <%@ Register
           TagPrefix="recaptcha"
           Namespace="Recaptcha"
           Assembly="Recaptcha"
   %>
   ```

   Then insert the reCAPTCHA control inside of the <form runat="server"> tag:

   ```
   <recaptcha:RecaptchaControl
     ID="recaptcha"
   ```

```
runat="server"
PublicKey="your_public_key"
PrivateKey="your_private_key"
/>
```

Public and private keys need to be substituted for specific keys. And these keys are provided from reCAPTCHA developers by clicking Create Key button on reCAPTCHA's website (https://www.google.com/recaptcha/admin/create).

5. Analyze form validation with Page.isValid method on submission.
   Following code with reCAPTCHA using Visual Basic is demonstrated analysis and check processes mentioned above:

```
<%@ Page Language="VB" %>
 <%@ Register
          TagPrefix="recaptcha"
          Namespace="Recaptcha"
          Assembly="Recaptcha" %>

<script runat="server">;
   Sub btnSubmit_Click(ByVal sender As Object, ByVal e As EventArgs)
      If Page.IsValid Then
         lblResult.Text = "You Got It!"
         lblResult.ForeColor = Drawing.Color.Green
      Else
         lblResult.Text = "Incorrect"
         lblResult.ForeColor = Drawing.Color.Red
      End If
   End Sub
</script>

<html>
<body>
   <form id="Form1" runat="server">
      <asp:Label Visible=false ID="lblResult" runat="server" />
      <recaptcha:RecaptchaControl
         ID="recaptcha"
         runat="server"
```

```
            Theme="red"
            PublicKey="your_public_key"
            PrivateKey="your_private_key"
            />

        <asp:Button
                    ID="btnSubmit"
                    runat="server"
                    Text="Submit"
                    OnClick="btnSubmit_Click" />
    </form>
</body>
</html>
```

3.3.3. Implementing security policies

The primary and most basic security tool of any organization is security policy. The security policy is the backbone of the entire operation because it defines the rules by which business is conducted. (Russell, 2000)

Following security policies should be applied to PillowHeaven

- **Password policies**

  Password policies ensure that passwords are sufficiently strong so that passwords cannot be easily guessed. The account lockout capability ensures that an automated scheme cannot make more than a few guesses before the account is locked. Password policies for PillowHeaven are displayed in the following text:

  - Shoppers have three chances to enter a suitable password. The account will be locked after shoppers or attackers have input the wrong password three times.
  - When shoppers set a password for their account, the password has to contain letters and numbers. The length of password should be more than 6 characters.
  - Users are advised not to store their password only in plain text directly into database. Passwords should encrypted by one-way hash algorithm before saving into database. I'll choose SH1 encryption as a one-way hash algorithm.

And will be added as a method to website utilities class with following code:

```
public static string CalculateSHA1(string str)
{
        byte[] result = new byte[str.Length];
        byte[] smth = System.Text.Encoding.ASCII.GetBytes(str);
        System.Security.Cryptography.SHA1CryptoServiceProvider sha = new
        System.Security.Cryptography.SHA1CryptoServiceProvider();
        result = sha.ComputeHash(smth);
        string strHashData = ystem.BitConverter.ToString(result);
                strHashData = strHashData.Replace("-", "");
                strHashData = strHashData.ToLower();
        return strHashData;
}
```

- **Other policies for future implementation**

  A comprehensive security policy is actually made up of several individual policies, each of which target unique lateral aspects of the site's business processes. The individual policies work together to provide three basic assurances for the site: confidentiality, integrity, and availability of data.

  Here follow some other individual policy examples that can be applied to PillowHeaven in order to manage and protect the system's security:

  - The sensitive and confidential data needs to be encrypted during the transfer.
  - Security experts can be employed to attack and analyze the E-commerce system regularly, so that the PillowHeaven can be updated according to the found bugs.
  - External security experts need to have verified appropriate processes and techniques of third party applications before installing them on the system.

  Different policies should be created depending on the type of the E-commerce network. It is of utmost importance to apply the policy. Administrators do not only need to understand all the policies, but also to apply the policy in the real work.

Furthermore, other departments of employees have to understand particular security policies according to their need.

3.3.4. Choosing suitable components and internet connection

It often happens that shoppers see a slow, unreachable, or not fully functional e-Commerce website.

What might cause that? One of the possibilities is that the network components do not handle sufficient volumes of network traffic. This section will discuss how merchants can use suitable components to work together and provide a stable working web site for shoppers.

Solving following conditions can be cause of well-functional e-Commerce system:

- **Determining the overloaded device**

  PillowHeaven infrastructure contains different components, which includes web servers, database server, financial transaction servers, DNS servers, and network equipments. If one of these devices works over their capacity, the whole application may not work properly. Sometimes, the overload device will work as efficiently as the device being down, but sometimes the overload device will work very slowly. Depending on the status of the overloaded device, the application will work slowly, or even not at all. The overloaded device is harder to troubleshoot than the device being down. For example, the most basic way administrators might use is a ping test to verify which device is not working. However, the ping test may not work for checking the overloaded device, since the overloaded device may still display "up" state from the ping test. To find an overloaded device, administrators need to understand each device's capacity and analyze which one is the current bottleneck in the whole network. As we know overloading is always associated with network throughput, CPU utilization, and what is in the RAM.

  Firstly, how can be determined the load of a router? Take Cisco routers for instance, it could be used to show interface to see the description of a particular interface. For instance, the command will show the particular interface, which is running 100Mbps, full-duplex Fast Ethernet. In addition, an administrator could use the command show

process to see the CPU utilization of the router. With description information, the administrator could decide if this router is suitable to work with other network components. Moreover, the web server is the most important component of the E-commerce network, so the administrator needs to consider if the web server has sufficient capacity to work with other devices. By checking the operating system of the web server, administrators may easily see a rough measurement of the overall load of a system. I'm only taking two of the most popular server operating systems as examples. In a UNIX operating system, uptime and top commands can be used to check load. Performance monitor provides a rough idea about what the load is and the task manager displays the CPU utilization to Windows users.

- **Managing Bandwidth**

  Bandwidth is one factor which may bottleneck an E-commerce network. When merchants buy an Internet connection from an ISP (Internet Service provider), they have to consider how much bandwidth the site normally needs. It is always good to find enough site bandwidth for customers, and the merchants do not need to pay much. There are two forms of bandwidth service merchants could choose. One is having the bandwidth delivered to the merchants' location, which means merchants will have their own connection line, which connects from merchants' site to the ISP directly. This form of service will be much more secure and convenient to the merchants. However, good service always costs more. For example, a common T1 Internet access is around $2,000 per month. How about the other option of service form? It is co-location which tends to be cheaper, but it is less convenient and secure. Since co-location allows many companies to share the cost of establishing bandwidth, the merchant pays much less than using his/her own line. How should merchants find a suitable connection for their E-commerce network? There many different software packages could monitor the usage of bandwidth, so analyzing the data may help merchants to make a decision. MRTG (Multi Router Traffic Grapher) is free software which monitors and measures the traffic load on network links as shown in Figure 3-10 below.

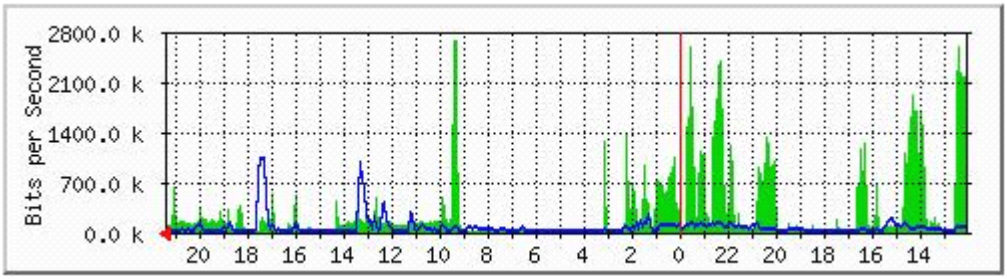

Figure 3-10 A sample MRTG bandwidth graph (adapted from MRTG)

3.3.5. Disaster recovery plan

If a site administrator configures a secure firewall, updates the latest patch for OS, uses secure software, and manages the whole network according to security policies, what should the administrator do if one of the servers is still down? How can the administrator find lost data from an unfixable server? A good disaster recovery plan may help the merchant to decrease that risk.

Basically, disaster can be classified in two broad categories which are: human-made disaster and nature disaster. Human-made disaster includes accidents, burglary, virus, intrusion, etc. Nature disaster is difficult to prevent, but with a disaster recovery plan, it is possible to decrease loss of data.

- **Backup rotation process**

  Since we never know when the server will be going down, and how much important data might be lost from a human made disaster, backup becomes a significant precaution, depending on the backup medium and how important the backup data are. Merchants could choose different methods to backup data.

  A full backup is very easy to understand, as the name implies, all the data will be copied to the backup medium after a certain period. Administrators copy all the data every day to the backup medium, so if a server is going down, the administrators will use the previous day's backup to recover the system. For example, administrators backup all the data from the system to the backup medium on Monday. The next day, Tuesday, the administrators backup all the data which includes the data comes from

Monday and Tuesday. In this way, there is maximum one day data lost by accident, and the whole recovery process will take place in a very short time. Of course, administrators may backup all the data in a period even shorter or longer than one day, depending on the backup plan. However, this method requires a lot of storage space media and time, since there are much data which may be repeatedly copied.

The incremental backup method solves the full backup disadvantage as it only records new data from the system to the backup medium. It saves much backup medium and time for site administrators, but it has some problems as well. For example, administrators use the incremental backup method to backup all the data on Monday as basic backup and the next day they only backup the new data which comes on Tuesday. The next day, the site administrator only records new data comes on Wednesday but does not record the new data which comes on Tuesday. In this way, it requires a very short time to copy the data from the system to the medium, and saves much backup space. When a server is down on Thursday, the administrators have to take backup data from Monday's record to Wednesday's record. If one of these days' backup is missing, this means that the recovery process will fail. Furthermore, this recovery process has to take a very long time to complete.

The differential backup is another method which combines those two methods. It contains two parts of data backup which are basic backup, and differential backup. For example, administrators copy all the data from the system on Monday, and they take these data as basic backup. On Tuesday, the administrators only copy the data which are different as basic backup. The same work will be done on Wednesday, so actually Wednesday backup contains the Tuesday backup and the new data coming from Wednesday but does not include the basic backup from Monday. If the server is going down on Thursday, administrators will need only two backup records which are the basic backup from Monday and the differential backup from Wednesday. In this way, merchants do not need to worry about the cost of the backup medium, and administrators could complete the recovery in a short time.

- **Off-site data protection**

Off-site data is the strategy of sending critical data out of the main location, in order to decrease the risk of losing important data from nature disaster, human accident or system crash. Normally, administrators have two options to send backup data away from its original location. One is sending those removable backup media to another physical place than the administrators' office. The other way is uploading data to an online backup system.

Carbonate is one of the companies offering this kind of online backup service to customers. More information can be found at http://www.carbonite.com/. And this service also can be used in order to protect data of PillowHeaven.

- **Building a redundant line to the ISP**

  As previously mentioned, the data needs to be backed up so that the loss from disaster is decreased. What else should be backed up in an E-commerce network? If the connection between the web server and the ISP is going down, then customers can not visit the web shop. This is a bad situation for merchants, since troubleshooting may take very long time. In the meantime, merchants will lose many potential customers. Building a redundant line with another ISP is good precaution for this case. When the original ISP connection is down, the redundant connection will take over immediately and replace the original one. If merchants cannot afford two network service providers, they could install two physical lines going to the same ISP as shown below in Figure 3-11.

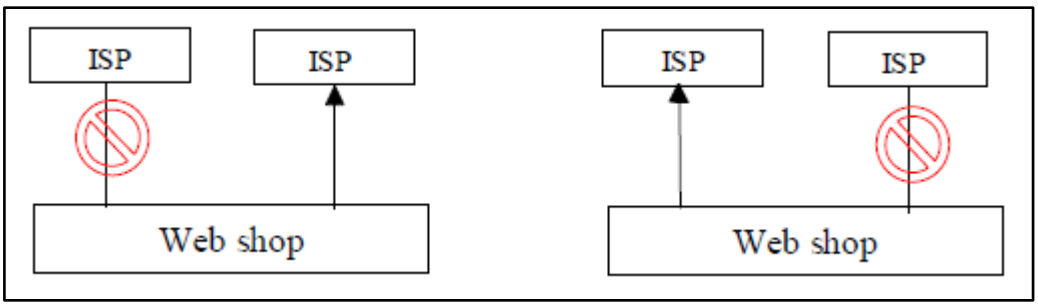

Figure 3-11 Redundant Line (Adapted from IBM)

4. Conclusion

There are lots of technologies such as firewall, SSL, monitoring site programs to protect the E-commerce. The technologies are developing faster than ever and thus the need for the merchants to take care of the software and hardware upgrades. The complacence in the upgrade of the system in time might result in system hack. So to prevent that the user on administration side must be given the security seminars from time to time. The implementation of a well-conceived recovery plan is necessary, so that we will be able to quickly restore the system after an attack. After the E-security and the policies have been realized it is necessary to act according to the policies identified to follow the security measures orderly. Otherwise, theory and plan will be only staying on the paper, and E-commerce will become a trouble maker rather than a good business platform.

The research that has been done for this thesis has certainly improved my knowledge and awareness towards the security measures that needs to be taken while trying to implement any E-commerce applications. And further my knowledge on the nopCommerce open source e-shop solution with N-tier application development has improved a lot.

5. References

1. OLKOWSKI David J. Jr., [2001] “Information Security Issues in ECommerce”, SANS GIAC Security Essentials.
2. WU Yan Yan, [2010]. “Engineering Materials, Energy, Management and Control, Advanced Materials Research, 171-172, 640
3. Anita ROSEN.[2002] “The E-Commerce Question and Answer Book: A Survival Guide for Business Managers”. 2nd edition. AMACOM. ISBN 0814471544.
4. Richard CONWAY, Julian CORDINGLEY. [2004]. “Code Hacking: A Developer's Guide To Network Security”. 1st edition. Charles River Media. ISBN 1584503149.
5. Michael SCHRNEK. [2007]. “Webbots, Spiders, and Screen Scrapers: A Guide to Developing Internet Agents with PHP/CURL”. 1st edition. No Starch Press; Annotated. ISBN 1593271204.
6. Milutinovic, Veljko. Patricelli, F.[2002]. “E-Business and E-Challenges”. Ios Pr Inc. ISBN 1586032763.

Internet sources

1. Van KETEL Mark and NELSONE Tim D., 2000. [Accessed on 8.3.2011]. [http://searchcio.techtarget.com/definition/e-commerce]
2. Wikipedia [Accessed on 8.3.2011]. [http://en.wikipedia.org/wiki/Denial-of-service_attack]
3. Scientific.NET [Accessed on 8.3.2011]. [http://www.scientific.net/AMR.171-172.640]
4. IBM. E-Commerce security: Attacks and preventive strategies. [Accessed in 8.3.2011]. [http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html]
5. ToonTownCentral. Computer Technical Support. [Accessed on 8.3.2011]. [http://www.toontowncentral.com/forums/computer-technical-support/202198-fake-emails-spoof-websites.html]
6. Digicert. IIS 7 SSL Certificate Installation. [Accessed on 8.3.2011]. [http://www.digicert.com/ssl-certificate-installation-microsoft-iis-7.htm]