Bachelor's Thesis (TUAS)

Degree Programme in Information Technology

Internet Technology

2015

Arun Sapkota

PRACTICAL DATA SECURITY TESTING ON A VIRTUAL LEARNING ENVIRONMENT

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Information Technology | Internet Technology

2015 | 39

Instructor: Virtanen Tero, Wikström Yngvar M.Eng

Arun Sapkota

PRATICAL DATA SECURITY TESTING ON A VIRTUAL LEARNING ENVIRONMENT

Data breaches in networks are a common issue in Internet Technology. Virtual environments are hidden most of the time, but academic working spaces need more security and encrypted space. This thesis focuses on issues arising at a virtual space created for a teacher for educational purposes.

The purpose of the thesis was to explore the vulnerabilities in virtual space in order to implement security patches in the future. Various hacking tools and penetration testing tools were used to discover the weak points left in the virtual space during the software development, which could be exploited by intruders. In order to find the security weak points, a security analyzer tool named Zed Attack Proxy was connected to the database server. It was given privilege rights and the database was evaluated with this tool. Subsequently, lists of possible weak points were generated and the thesis discusses these weak points and proposes possible solutions.

KEYWORDS:

Penetration, database, Intruders, SQL, Iron WASP, W3af, virtual learning environment.

CONTENTS

TABLES

FIGURES

LIST OF ABBREVIATIONS (OR) SYMBOLS

ASP	Active Server Page
CD	Compact Disc
CPU	Central Processing Unit
DMARC	Domain-based Message Authentication, Reporting and Conformance
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GWS	Google Web Server
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IIS	Internet Information Service
IPS	Intrusion Prevention System
IT	Information Technology
NT	New Technology
OS	Operating System
OWASP	Open Web Application Security Project
PGP	Pretty Good Privacy
PHP	Hypertext pre-processor
RTF	Rich Text Format
SMTP	Simple Mail Transfer Protocol

SQL	System Query Language
SSH	Secure Shell
SSN	Social Security Number
TLS	Transport Layer Security
URL	Universal Resource Locator
VLE	Virtual Learning Environment
W3af	Web Application Audit and Attack Framework

1 INTRODUCTION

With the advancement of technologies, the internet is routinely usedin the academic world. The internet has transferred the academic platform from the classroom to the digital world in the form of ‘e-Data'. Data is supposed to be less secure when it is exposed to the internet rather than inside the internal network. When information is revealed on the internet, it becomes visible to a global audience and is threatened by various factors. Thus, data is stored, shared and managed with updated security measures so that anonymous and illegitimate users can not access it. Potential security threats for the data have never been an easy topic for IT decision makers. As defense matures, the frequency of threats exponentially increase. The more the confidentiality increases for the data, better the security measures should be.

This thesis deals with a project based on data security, exploring the breach points and various practical methods which could help to update the client appliances for further security improvement. However, the study based on the client’s environment raises various issues of breaches in network and reveals the weak points of the system. Mainly, the thesis is focused on finding a solution to the following :

- recognition of breaches in the system and the network
- Discovery of future potential threats and attacks
- implementation of a solution minimizing security risks
- Generation of RSA-keys, protocol implementation to a secure database and network.

By using various tools and software, the problem will be analysed to obtain an idea of the nature of the problem. The basic question is to safeguard the original software while checking the hacking tools. Penetration tools shall also be used for listing out the problems.

The primary goal of the thesis is to research the code and software to discover the weak points and vulnerabilities in order to find the solution so that no attack can be reported from intrusion with malicious code. In order to achieve the objectives, the Server Query Language (SQL) Management Studio will be used to explore the tables and views. In addition to that, the penetration tool, OWASP will be used to find the breach point and possible solution to make the database and web interface secure and robust.

2 VIRTUAL LEARNING ENVIRONMENT AND ITS ADVANTAGES

A Virtual Learning Environment (VLE) is a web-based learning technology, which helps to implement the learning of knowledge in and beyond the four walls of classroom. In this century, VLE has been the one of the most successful methods of learning among the educational institutions. Generally, a VLE includes course contents, learning materials, planning of the course. Usually a VLE is not made for specific course or studies, it may include several courses and their learning materials.[1] VLEs may differ from one to other because they are tailored to the needs of the users and are comprised of different extra features such as: e-mail, wiki, blog, discussion rooms, presentation slides, notices, learning diaries etc.[2]

A VLE can be a web application provided by the faculty (OPTIMA) or could be self-made, open source application (MOODLE) or can be free in the web.

Mainly the advantages and features of VLE can be summarized as follows[3]:

- Students can have access to learning materials, such as presentation slides, notes, email, discussion, wiki, blog etc. from anywhere but they have to keep in mind that they must follow the proper process to access it otherwise the permission will be denied.
- It helps to maintain the mutual interaction and good communication between the teachers and students.
- It helps students to have control over place, time, pace and path which could be helpful in their study.
- It could be one of the factors for students to develop the passion of learning.
- The presence of interactive and user-friendly application in VLE could make student making learning personal and engaged.[4]
- With the help of VLE, students can track their progress.

3 DATA SECURITY

Data security is a preventive measure which is applied to prevent the data from unauthorized user access to the computer, database and websites. It prevents the sensitive data information being stolen, deleted, or changed. Commonly used technology for data security is the password authentication that consists of username and a strong password. One of the main technology measure for data security is encrypting where the data is encrypted with mathematical schemes and algorithms in order to make it unreadable to hackers. Every platform that uses the database system should be aware of data security in order to have a proper database management system.

3.1 Data Classification

In order to maintain proper security, data classification plays a important role in it. Data classfication helps administrators choose the apporiate security measure that should be applied in order to prevent data from unauthorised access. Normally, data are classified on the basis of their importance and impact in case of theft . Mainly data are of three types[5], which are as follows :

- Confidential Data

Confidential data refers to information which is highly restricted from public access. Confidentiality can be defined as the set of rules that gives the limited access to the data. It is one of the main components of data security. The disclosure, change and loss of the confidential data without the authorization may lead to huge losses forthe owner. Higher level of security precautions should be applied to these types of data. Social Security Number (SSN), Medical Information, Exams and Answer keys, Bank Credentials etc. are considered as confidential data as they require highly restricted security outbound to prevent illigetimate access and exploitation. Hence, publicly restricted data requiring high-level security boundary is termed as confidential data. [6]

- Private Data

Private Data can be defined as the internal or some organization/company's data that are not suitable to disclose to the public.In simple definition Those data which are not assigned as restricted or for public access is known as private data. The disclosure of this kind of data may lead to a moderate level of risk to the organization. The medium level of security measures should be applied to this kind of data. Examples of private data could be company sales reports, organization details etc.

- Public Data

Public data can be defined as the data which could be easily accessible by the public without any restriction. The alternation of these kind of data does not make any or may cause little physical or financial impact to the owner. Public data only requires the basic level of security measures only to prevent the unauthorized user to alter the data. Examples of public data could be the public websites, course descriptions in a VLE etc.

3.2 Applications of Data Security

With the advent of new technologies, more threats are emerging for data security. Hackers and crackers are coming up with much more sophisticated means of attacks. Digital communication has made the data transfer and data communication very fast, easy and efficient. Data protection and integrity is of essence to both customers and companies. This section describes the major applications of data security.

1. Encryption: The process of converting data into unreadable forms to protect the data is called encryption. Messages or data can be encrypted using different encrypting algorithms that can only be read if decrypted. There are many different types of encryptions available. Listed below are the major encryption types :

- Symmetric key encryption (Using the same key to encrypt and decrypt the message)
- Asymmetric key encryption (Using different keys to encrypt and decrypt the message).

Seventy one percent of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage (Computer Security Institute 2007). Encryption can be used to encrypt files that are stored at storages devices. In addition, it can be used to encrypt the data that is transferred over the network so the data can be protected from man-in-the-middle attacks or eavesdropping.

Information or data is the one of the important factor in modern web technology. Data can be protected in various ways and encryption is a popular method. There are three basic encryption methods availllable, which are as described below :

- Hashing Encryption
- Symmetric Encryption
- Asymmetric Encryption

Depending upon the type of encryption method, each has its own importance, disadvantages, and uses. Encryption depends upon cryptography. The use of encryption method ensures that the message that has been received or sent, has not been altered or deleted during the transit and helps to verify the identity of the original sender. All of these benefits can be achieved with the use of the above metioned encryption methods.

- Hashing Encryption

In the hashing encryption method, a message or set of information is provided with a unique and fixed-length of the signature. Generally, hashes are made up of the hash function or algorithm, which is used to compare the set of information. Hence, a small change in message results in a huge difference in hash, because each hash is always unique to the specific message.

If we compare all three encryption methods, the unique difference that the hashing method possesses is that once the message or data is encrypted, the process is irreversible. This means that if a hacker sucessfully gets to the hash, he or she is not able to decrypt the data to view the original message. Some of the commonly used

hashing algorithms are the secure hashing algorithm (SHA) and the message digest (MD5).

Drawbacks of Hashing encryption

Although its impossible to undo a hash, it is possible, with access to the hash, to find data that hashes the same as the password. Thus, it is always encouraged to use strong password to make password-hashing algorithm effective.

- Symmetric Encryption

Symmetric encryption, also called private-key cryptography, is most secure encryption and is one of the oldest methods of encryption. The term private key comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone who has access to it can read the encrypted messages. A key is used to encode a message into a ciphertext, and the receiver uses the same key to decode it.

This encryption is used as a method of either a stream/block cipher which depends on the amount of data that is being encrypted or decrypted at a given time. A stream cipher is used to encrypt data one character at a time as it is sent or received, while a block cipher encrypts a fixed amount of data at a given time. Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA) are some of the commonly used encryption algorithms.

Drawbacks of symmetric encryption

- If it is a password, then the user needs to type that password every time the software starts up, this is the basis of how disk encryption works on personal computers, like Mac OS X is FileVault 2.
- If a user has to store the key on a disk or a device for example in an application, or to transmit it without encryption over a network, the encryption is useless once an attacker gains access to the key.
- It is also important to remember that software needs access to the unencrypted data to do its job even if the data is encrypted, meaning that the encryption

once again becomes useless if the software or platform itself is compromised. The only way to effectively protect against this is to design the services in such a way that as data leaves the user's computer, it is encrypted, leaving the key exclusively in the user's possession and storing only unreadable encrypted data. However, this reduces the usefulness of many systems that may need to read the unencrypted data to function.

Uses of symmetric encryption

The common uses of symmetric encryption are listed as follows:

Symmetric encryption is used

- In services (like cloud backup services) which store encrypted data for a user when those services leave the decryption key in the hands of the user.
- To encrypt computers or storage devices (One particularly neat property of a well-encrypted device is that it can be quickly erased. The resulting encrypted data still stored on the device is then useless to anyone).
- To create a secure channel between two network endpoints, where there is a separate scheme for securely exchanging the key.

  If used properly, symmetric can be very effective, however the key needs to be protected even while it is being shared among the parties that legitimately need it.

- Asymmetric encryption

Asymmetric encryption, also called public key, is far more secure than symmetric data encryption. A private key and a public key are used to perform this kind encryption and decryption. This use of two keys overcomes one of the greatest weakness in symmetric key cryptography, because a single key does not need to be managed securly among multiple users.

A public key is entirely public and available to everyone and it is used to encrypt messages before sending them. The other key, the private key remains with the receiver of the ciphertext messages who uses it to decrypt the message.

Drawbacks of asymetric encryption

There are caveats to asymetric encryption. One of the most challenging issues with public-key cryptography is making sure that the users can trust the public key they have. Man-in-middle attacks are one of the most common ways to compromise asymmetric encryption. The user is given a public key to use to securely communicate with service, and dutifully use it, thinking it is safe. However, through network trickery, the user is communicating with another party sitting between the other end and the user.

The third party in the middle gives the user their own public key, and gives another public key to the other user, pretending to be the first user. Thus the user in the middle can decrypt the first user's data and encrypt it again and send it to the other user and vice-verca to gain full access to the unencrypted data. Protection against this kind of attack is accomplished by making sure to have the right public keys, either by having entities we already trust cryptographically sign new keys or by distributing them in trusted software.

It is therefore important to acquire a certificate for the user's HTTPS site from a certificate authority which is trusted by web browsers.

Uses of asymetric encryption

- Asymmetric encryption is pervasive on the Internet. In fact, Internet would not work securely without asymetric encryption.
- It is used along with TLS to secure connections between the browser and the website as well as other services in network.
- It is used with SSH to secure login sessions to remote servers.
- It is also used to sign software updates so that computers and devices know that they are getting the information that originated from a party that can be trusted.
- It is also possible to use asymmetric encryption for email with systems like OpenPGP or S/MIME .

3.3 Positive Impact of Data Security

Perhaps the most striking impact of data security comes into play when we talk about online platforms like learning virtual environment, online shopping, banking systems etc.

For example, it seems impractical to imagine a bank website without proper data security measures, thus requiring complex security architecture to be implemented to guard data traffic. In the age where phising, social engineering, and theft attacks are major threats for data architecture require major a security component in network . Thus, security protocols and measures are essential in securing data to eliminate intrusion holes in complex data rings.

Furthermore, modern methods are being implemented in securing data and letting users to explore it in safe and secure online environments. For instance, the area of this thesis project is a virtual learning environment where students access study material and expect the environment to be secure although threats, such as man-in-the-middle attacks, are more likely to happen,. Mostly, intruders wait for security issues and exploit vulnerabilities to benefit and steal data.

Similarly, cellular networks is another place where data security is of immense importance. Had it not been for the security protocols and user data encryption, the voice and other data of user along with the user's credentials would have been at risk. The result would have been identity theft, data stealing and compromising the privacy of the user data. This would have naturally been a cause of chaotic state and that is why mobile companies invest so much in data security.

3.4 Popular Data Theft Incidents

Hundreds of data theft incidents are reported every year, as part of various network attacks. Hacking tools, threats and other means could be media of these breaches. Moreover, thousands of data theft occurred at lower level are unreported. The latest popular data theft incidents around the world are listed in Table 1[7].

Table 1. Popular Data theft Incidents.

Date /Company/Total loss	**Data theft Incident**
March 2008 Heartland Payment Systems 134 million credit cards exposed	Culprits were accused of fabricating a theft that resulted in stealing bank card data. The basic issue was SQL injection, which was the most vulnerable security hole in most of the web-based attacks.
December 2006 TJX Companies Inc. 94 million credit card attacks exposed	According to one group, weak encryption was the main reason behind this where credit card data was stolen when the data was being transferred wirelessly. Another group mentions the absence of firewalls in Kiosks was the main reason.
March 2011 RSA Security 40 million employee records stolen	The incident where the sensitive information is stolen from the company is secured using authentication token systems. Two hacking groups backed by Foreign Government carried out phishing attacks against employees as the possible entry point to company's network. The main lesson learnt was that even security companies are not safe against such attacks.
April 20, 2011 Sony's PlayStation Network 77 million PlayStation Network accounts hacked; financial losses accounted to be in millions	Perhaps the worst breach in gaming industry that the world has yet seen as 77 million accounts were affected of which 12 million had unencrypted credit card numbers. To this date the hacking group has not been found according to Sony officials but they gained access to users' data that was on Sony's servers. One possible reason according to Sony was the possible misuse of the user's data on users part.

3.5 Intrusion Holes Left During the Software Development

Activities on the internet performed by anonymous communities in order to weaken integrity, confidentialy and resource availability for the network users, are popularly known as Intrusions. They generally acquire authorized access by exploiting vulnerabilities. This can be possible though various means, such as Protocol abuse, holes left during protocol implementations. Basic media of popular intrusion detection system is the Synchronize (SYN) scan, because sometime IDS can not scan popular threats.

The latest intrusion holes found are termed as black and gray holes[8], which disrupt routing in ad hoc networks based on cross layer design. Most of the time, a black hole attack is performed by issuing malicious code which tries to acquire a route source to destination by referencing a false number and hop count in the routing message.

In order to detect and prevent these kind of attacks, various effective IDS nodes are deployed in sniff mode to trigger a mechanism called Anti-blackhole mechanism. When a suspicious value is greater than the normal node, there is abnormal difference resulting in routing messages transmitted from node, broadcasting a block message.

Recent example

A 21-year old hacker peered into the database residing in the intranet of The New York Times Co. and patched an intrusion using web browsers. As it was reported from an official article of the newspaper, he accessed the company's database in order to retrieve information, such as subscriber names, correspondence, editorial contact names, addresses, and phone numbers as well as social security numbers, although financial information were not available.

4 DATABASE AND WEB SERVER SECURITY

The Project explains the major data threats found by scanning through tool called Zed and possible solutions, that could be implemented.

4.1 Major database servers

A database server can be defined as an application that uses client/server artichecture to peform tasks such as data storage, manipulation of data, data analysis etc. The database server can be accessed with the help of different applications. Database servers differs from each other in the way they store data and the way they allow multiple users to access the information.

Some popular database servers are listed as follows:

- Oracle
- DB2
- Informix
- Microsoft SQL server
- Sybase
- PostgreSQL

4.2 Advantages and limitations of Microsoft SQL Server server

The project implies on the server based on Ms-SQL-Server, having advantages with few limitations, comparred to (ex-Oracle). Besides this, it is open source framework which allows copy, modification and re-implication.

Advantages of SQL Server

- The SQL server provides the security features and can be managed in all database objects such as table, view etc. It provides strong password authentication features and enforces to change of password quite frequently.
- Use of Data Encryption is one of the main advantage of it.
- In terms of scalability, the SQL server is highly scalable which allows for managing petabytes of data.
- The SQL server offers different availability features such as database mirroring, log shipping and database snapshot as per need.

Limitations of SQLServer over its Competitors (ex: Oracle Server)

With the popularity and exponential rise of MySQL users, the SQL server is implemented by various organizations.

Like every other database, it does have disadvantages which are described below:

- Various database servers like SQL and Kerberos, MySQL show unrelated linkage into Active Directory.
- Even MySQL doesnot have dependency on check constraints.
- It does not provide debugging and developing tools for developers, hence, complicated codes cannot be resolved, if bugs arise.
- The absence of standard encryption inside a stored routine provides space for intruders to exploit vulnerability.
- MySQL can not work efficiently with huge databases, and can not perform transactions.

4.3 Major web servers

The main purpose of a web server is to store, process and deliver the requested webpage to the clients. As technology is growing tremendously, the number of web servers is also increasing.

Below are the some of the most popular web servers:

- Apache
- IIS
- Nginx
- GWS

4.4 Advantages and limitations of Internet Information Server (IIS)

IIS supports FTP, FTPS, HTTP, HTTPS, SMTP and NNTP. IIS provides a platform for secure hosting websites, application and services. IIS with Microsoft consists of a set of programs for building and administering the websites, the applications and the search engines that can access the databases.[9]

Advantages of IIS

- It is user friendly and can be downloaded free from the web including the Microsoft Web Platform with frameworks, database and development tools.
- It supports programming languages from ASP.NET to PHP and provides a strong and manageable web server. Popular application such as WordPress, Umbraco and Drupal can use the IIS server.
- Adminstrators can customize and add new features using the IIS Extensions.
- It increases the web server security by default with less Web server footprint and automatic application isolation.
- It will speed up the performance of a website through dynamic caching and advanced compression. It fastens the performance of both static and dynamic Web with the help of HTTP compression and integration from Windows Kernel for SSL Websites.

Limitations of IIS compared to the Apache Server

- IIS is intended for Windows systems only whereas Apache runs on almost every OS.
- As IIS is for Window systems, Windows is also known as the system that has more chances to suffer malware attack and is recognized as a less secure server option.
- IIS is being supported by Microsoft whereas Apache is supported by the open source user community.
- Concerning its operational cost, it is more expensive than Apache due to the necessity of Windows OS only.

4.5 Common threats in web servers and database servers

The database system is called the heart of the organization as it stores all client information and contains the confidential data that might be useful to the hacker in order to gain access to different platforms. In order to secure the data, The server needs to be secured. One of the common threat related to the database server is the SQL injection

SQL injection

SQL injection refers to the attack in which an attacker injects an intrusive SQL statement in the query field in order to dump the database content of the client system. If the SQL injection is succeful, it can incurs changes in the database system and can even gain access to the administrative operations on the database. The SQL injection takes place using malicious scripts in the field of user input, leading to major database errors.[10]

4.6 Best practices to minimize common threats in database server and web server

In order to secure the server firstly, the network needs to be well shielded. Attackers always have the intention to find intrusion holes in the network in order to gain access to the server.

The following methods are best practices to minimize common threats in database servers and web servers[11] :

- Nowadays, hackers are well versed in inventing new viruses every single day. In order to prevent the system from those kinds of viruses, it is necessary to keep the antivirus software updated. Out of date antivirus software can allow for new virus attacks.

- The use of DMARC software can also be the one of the preventive measure against email threats. DMARC software notifies the administrator of phising and malware threats in thesystem. If any unknown IP addresses or URLs are trying to gain access to system, an alert message will be issued to prevent further damage.

  According to the DMARC security expert in the Agari blog post[12] “In most cases,the criminals have compromised a website such as blog and cropped their phising kit into it. A phishing kit is a pre-built version of the corporation’s website that they can drop on any web server, in order to impersonate the company.”

- A strong password policy could also be one of the best pratices to secure the server. Generally, most of the security systems use passwords as the keys to provide access to the data and information in organization. A strong password policy protects the system against cracking and guessing passwords threats.

5 DATA SURVEILLANCE AND IDENTIFICATION OF THREATS

Data travelling through external traffic needs regular monitoring and surveillance so that the network adminstrator can be notified of unusual behavior. There are plenty of tools and software which are mostly installed on the network either on server side or the client side to detect anamolous changes and behavior, and to minimize risks.

5.1 Ways of Data Surveillance

Threats to data can be minimized through various encrypted and unencrypted methods implemented for surveillance, achieved through legal or illegal monitoring of data over networks.

Surveillance aids to minimize threats, reduce criminal activities and control misuse of authorization of access controls. In most of the reported cases, threats arise from inside the network by misuse of access data. In order to reduce these cases, the following methods could be used for data surveillance:

1. Packet Capture: Data is monitored through each communicated packet over the network. Various packet capture appliance software are installed on the network to analyze traffic. Huge usage of the internet has crowded the web, thus increasing risks to data in form of various threats.

2. Social network analysis: Internet traffic is analyzed based on social network data such as interests, friendships, beliefs, affiliations, thoughts to investigate threats in any network.

3. Policeware and govware: Various policeware and government software are used, nowadays to examine the data through Internet service provider networks to keep updated logs of data flow. In case of doubtful or trojan data, it is assessed for further verification.

5.2 Types of threats

Data security threat has become the one of the challenging topic in the world. The majority of the consequences arises by exploiting vulnerabilities by hackers who develop modified code and exploit the network to corrupt data and crash the system.

Based on the impact and area of effect, these threats are categorized as follows:

5.2.1 Social Engineering

Social engineering is a psychological manipulation of a person to perform a routine task. Normally, social engineering is performed in order to break the security bridge between the secure network and the attacker. Virus writer, phiser, scareware use the social engeering tricks on people in order to get a successful entry to the system and network.

- Phishing

It is a type of attack in which a attacker sends an email that direct receiver to a website which looks like a legitimate source but is managed by the hacker in order to gain private information details such as: bank account number and credit card details. Usually phising email redirect receiver to websites such as banks, Paypal, Amazon where receiver need to enter the banking credentials.

- Pretexting

Pretexting is the type of social engineering attack in which the attacker wins the trust of the targeted individual by pretending to be someone else and will access personal information, such as social security number, address, and date of birth. Normally the attacker will ask a series of questions which the targeted person will answer and the attacker will use this information to get access the system.

- Spam

Spam is an electronic unwanted, junk, bulk, and unsolicited email that is sent to numerous users frequently in the form of commercial advertisment for a certain product or service. Usually this type of junk email would be the bridgehead for the other type of social engineering attacks, such as phishing, email scams, pretexting etc. The best way to avoid spam is to use email software that has spam filtering.

- Baiting

Baiting is the attack that is comprised of the physical media such as CD-drive, floppy disk, flash drive, memory card etc that are affected with the malware. The attacker knowinly leaves that type of infected physical media in a place where the targeted person would be able to get that. As soon as target person inserts the media into their computer, then victim would see the content and unknowingly install malware on his system which would allow the attacker to access the targeted system.

5.2.2 Physical threats

Physical threats always makes a network more complex due to implementation of various secure socket layer protocols and security softwares like Firewall and IPS/IDS. It is true that it redefines network traffic and assessment. In addition, it adds load to the traffic and resources. Data flowing through the network needs checkpoints, which would assess each packet and only allow legitimate packets to pass through, dropping anonymous packets.

Data stored in digital media and hardware are exposed to a wide number of internal and external threats that could be minimized with timely attention and proper measures. This list of physical threats include:

- Hardware malfunction and improper maintenance
- Infrastructure failure and malfunction
- overuse of physical connection to hardware
- human errors as well as improper handling of devices
- vandalism of infrastructure and storage devices of data
- hacked with unauthorized users and modified
- deleted or altered by internal employees within organization
- damaged with reason of faulty drives, malfunction power etc.

5.2.3 Online threats

Online threats refers to the attacks that use the internet to gain access to sensitive data using different types of malware which may use the HTTP or HTTPS protocol or other protocol along with components, like email, advertisement attached to malware or even server. Basically, until today there have been many online threats that can easily affect computer systems but among all of them the following are quite popular[13]:

- Trojan horse

Trojan horse is a software that can get into thecomputer either by pretending to be trusted but in reality it contains malicious threats or is installed secretly while downloading the free software that are available in web. It is supposed to alter the data in computer and can also record keystrokes to access usernames and passwords.

- Virus

Computer virus refers to the malware program which replicates itself when executed into the computer programs, hard drive, and data and often in the boot sector. Once the virus enters into the computer system, it performs various harmful activites such as stealing confidential data, consuming the CPU time and hard drive space, corrupting data etc.

It can also watch over the keystrokes of the infected host in order to gain access to the different system and may also result in the system failure. Sometimes, it is also used to spy on the detailed security system that is applied in order to protect the data and send that information to the virus writer. Normally a virus enters into the system through the use of different web activities, such as visiting an infected website, downloading free games, music, video or system utilities. The use of antivirus protection and a firewall, keeping the OS up to date, increasing the browser security can be helpful to eliminate the computer viruses.

- Worms

Similar to viruses, worms are self-replicating computer programs which contain the malicious codes that are intended to penetrate in OS and create a network security holes for other application which may leads to Denial of Service (DoS) attack. The main difference between the viruses and worms are the methods they spreads to the

computer system. The use of validate antivirus application is the best measure to stop the worms.

- Brute force attack

A bBrute force attack is a cryptanalytic attack which is targeted to the system which has maintained low security in its encryption. Basically, it checks all the possible keys or passwords until it suceeds to gain access to the targeted system. In this case, passwords with short length can be easily guessed whereas long length passwords need other techniques. Due to this attack, the performance of the server goes down and may even run out of the memory.

5.3 Risks of threats

Various data threats have been reported till date, with various risks in commercial networks. Risks of threats include:

- Excessive and Unused Privileges
- Denial of Service
- Malware
- SQL Injection
- Identity sniffing
- Accidental access or changes
- Inject packets
- Server compromises
- Digital theft
- Spoofing
- Data theft and data destruction
- Software theft and compromise
- Eavesdropping and intrusion attacks

- Impersonation
- Social engineering and network spoofing

5.4 Techniques involved in minimizing risks

Threats arise with network complexity and vulnerabilities are exploited by accessing illegitimately through intrusion holes left during software development. These could be inefficient codes or insecure network. The following methods can be applied in order to minimize risks:

- Timely identification of vulnerabilities with penetration testing and various scanners available.
- Making a network robust with firewall implementation and IPS/IDS[14, 15]
- Less physical access of authorized people to the server.
- Encryption and other security measures should be adopted.
- Patches and extensions should be upgraded as per the need of workspace.
- Less exposure of the backend system
- If a system is compromised, a better solution should be applied to prevent future risks
- Analyzing and assessing risk to implement security solutions to stop unauthorized access to the server data.

6 PROJECT RESEARCH AND IMPLEMENTATION

The Virtual Environment deployed in this thesis project is based on a university learning space which was assessed to explore intrusion risk and vulnerabilities. The purpose of this thesis project was to make it more secure and safe for students and staff members as well as in order to protect their private data and critical information. However, it requires general understanding and research into on current configuration that could be applied during the testing procedure.

Microsoft SQL server Management Studio 2012 was used to explore the SQL database tree structure[16]. Figure 1 illustrates the outlook of database tree in SQL Management Studio 2012.

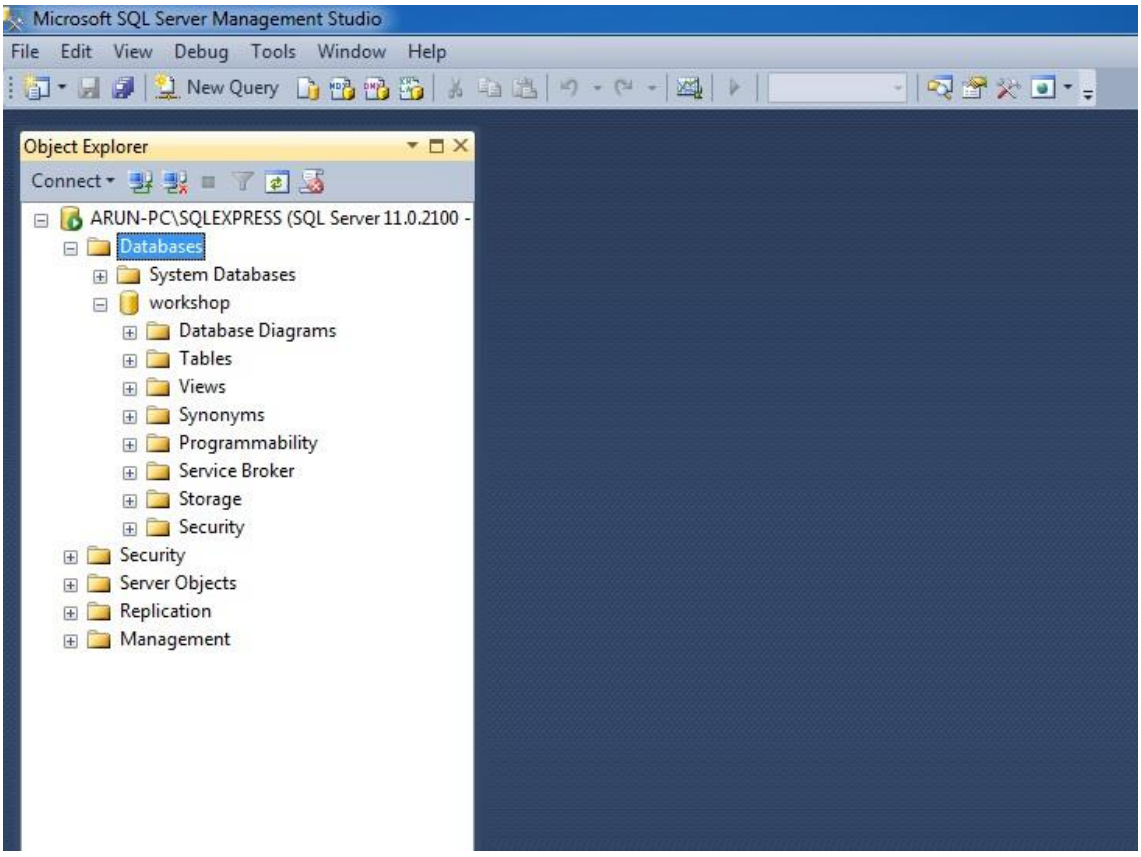

Figure 1 . SQL server Management Studio 2012

Workspace security assessment

A huge number of assessment tools are available in Internet. Many of them could be used in order to discover the vulnerabilities in legitimate websites. In addition to that, assessment tools also help to apply a solution to avoid defined problems for preventing future risks. A timely implemention of solution over the security holes prevents server down-times and network crashes for users.

After reasearching into assessment tools, the following tools to discover vulnerabilitieswere identified[17]:

- Wireshark
- W3af
- Zed Attack Proxy
- IronWASP

These tools are used to test the area of weakness in software trees which is known as penetration testing. The following steps were followed in order to carry out penetration testing:

- Issues causing errors and bugs were listed in priority order.
- The targeted system was attacked from both inside and outside in order to check access to the data, network, and server.
- The system was attacked and whenever accessed with unauthorized access, steps were repeated.

Penetration testing is carried within the network, servers and websites by testers or security professionals. One of the error message observed on the VLE website is shown in Figure 2.

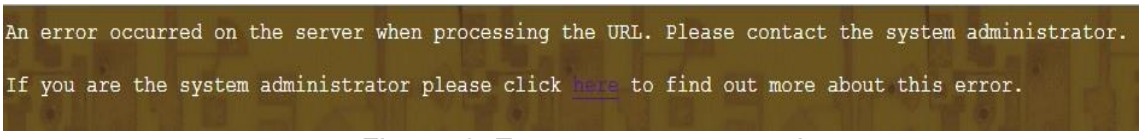

Figure 2. Error message reported

Wireshark

Wireshark is an open source software that is used for network troubleshooting by providing the detailed information about network protocols, packet data etc. It is multi-platform compatible. It can be downloaded from the official Wireshark page i.e., (https://www.wireshark.org/)

W3af

W3af is also an open source web application that scan the vulnerability and exploitation in web-based application and also provides the detailed solution that needs to be taken in order to prevent the vulnerability. It is compatible with most of the OS such as Windows, MAC OS X, Linux etc.. It is developed using the Python language which made it easy to use and extend. It can be downloaded from the official website, i.e. (http://w3af.org/)

Zed Attack Proxy (ZAP)

ZAP is also an open source web application that is intended for both beginners and professionals in penetration testing in order to find the intrusion holes in application. It was also voted as the second top security tools in2014 .ZAP is written in Java and run on multi-platform OS. It can be downloaded from the official site, (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project#tab=Main)

IronWASP

IronWASP is also a free and open source web security scanner that is entitled to automatically find the security issue on website. It is easy to use and also compatible with most OS. The features also include the reporting of the vulnerabilities in both HTML and RTF formats. It can be downloaded from the official website,

(http://ironwasp.org/download.html)

Since the VLE database was installed at a local machine, it was comparatively easy to find bugs and have them fixed, but, on larger scale it was not tested for its further response.

Based on the tests with the penetration tools, the following bugs were reported:

- Application error disclosure

An error message was displayed concerning the disclosure of the sensitive data which may lead to the further attacks against the web application. Interface appears as shown in Figure 3.

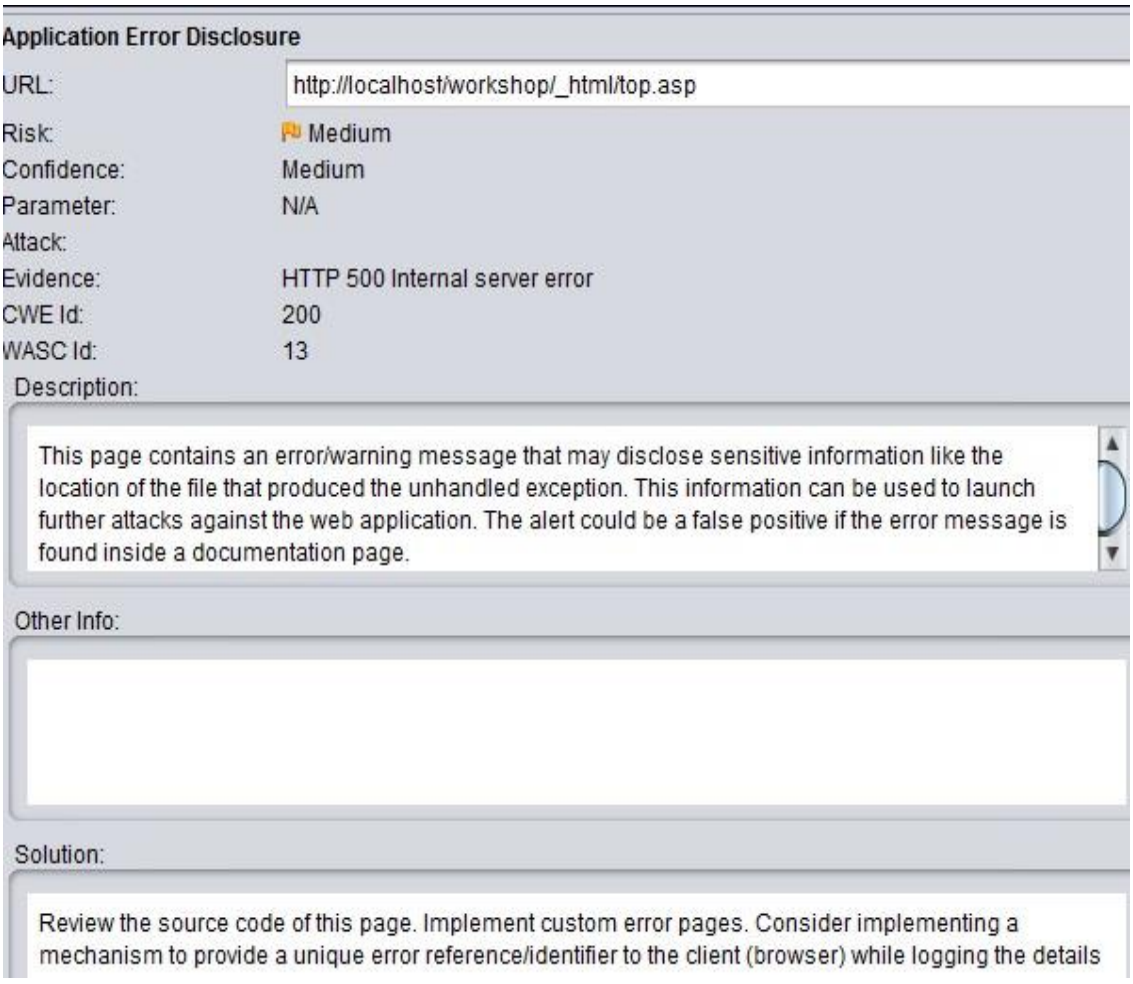

Figure 3. Application Error Message

Solution

In order to fix the application error message bug, the solution found was tomodify the source code of the page. In order to hide the server side information, it is necessary to implement custom pages by providing unique reference to the browser, everytime users log to the server.

- Lacking X-FrameOptions Header

There was problem with X-Frame-Options header in HTTP which is supposed to prevent the system from 'ClickJacking' attacks. The bug reference in bug discovery tool is shown in Figure 4.

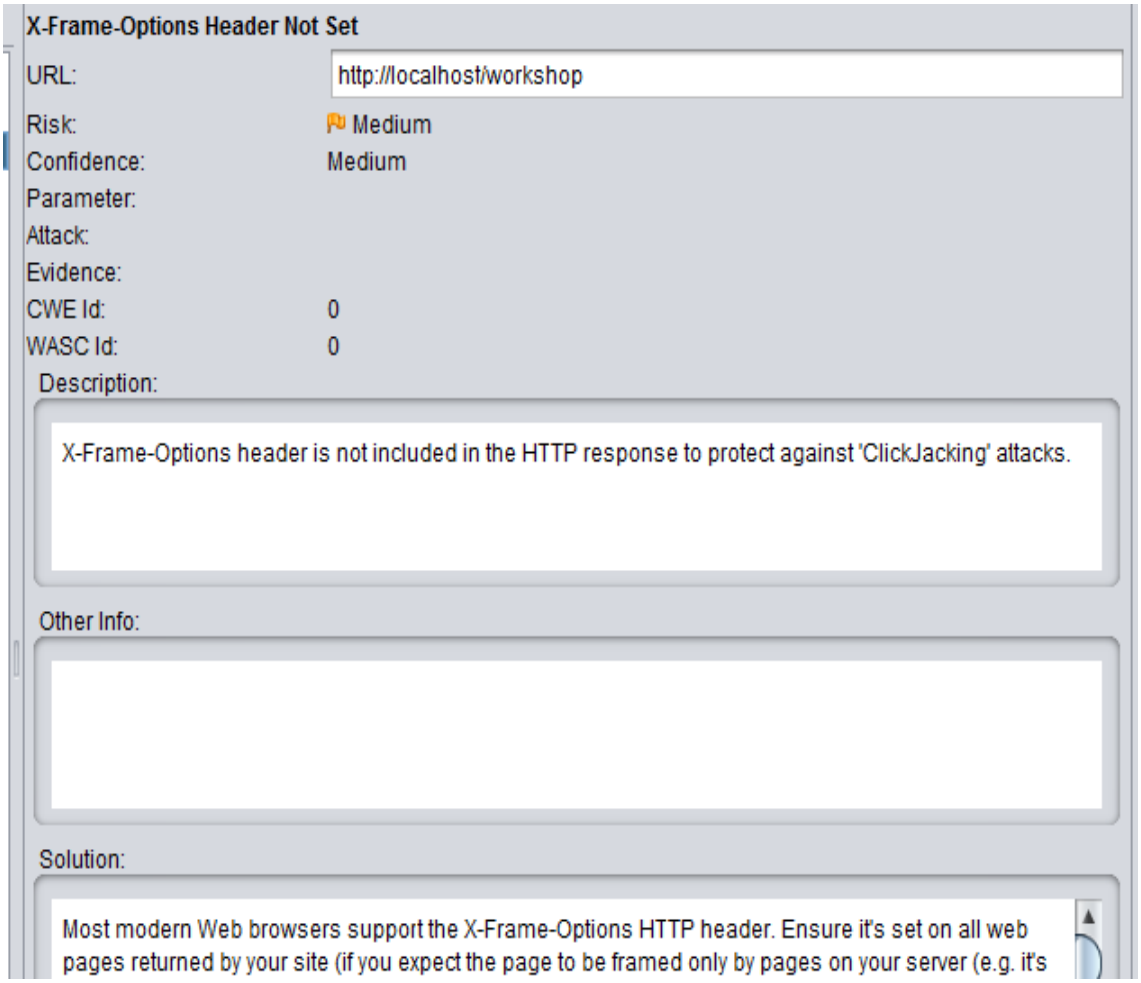

Figure 4. X-Frame Error message

Solution

The appropriate solution was to use of X-Frame-Options HTTP header because most browsers are compatable with it .

- Web Browser XSS Protection not enabled

The web browser XSS was not set or was disabled on the configuration in web server. The web response in bug discovery in shown in Figure 5.

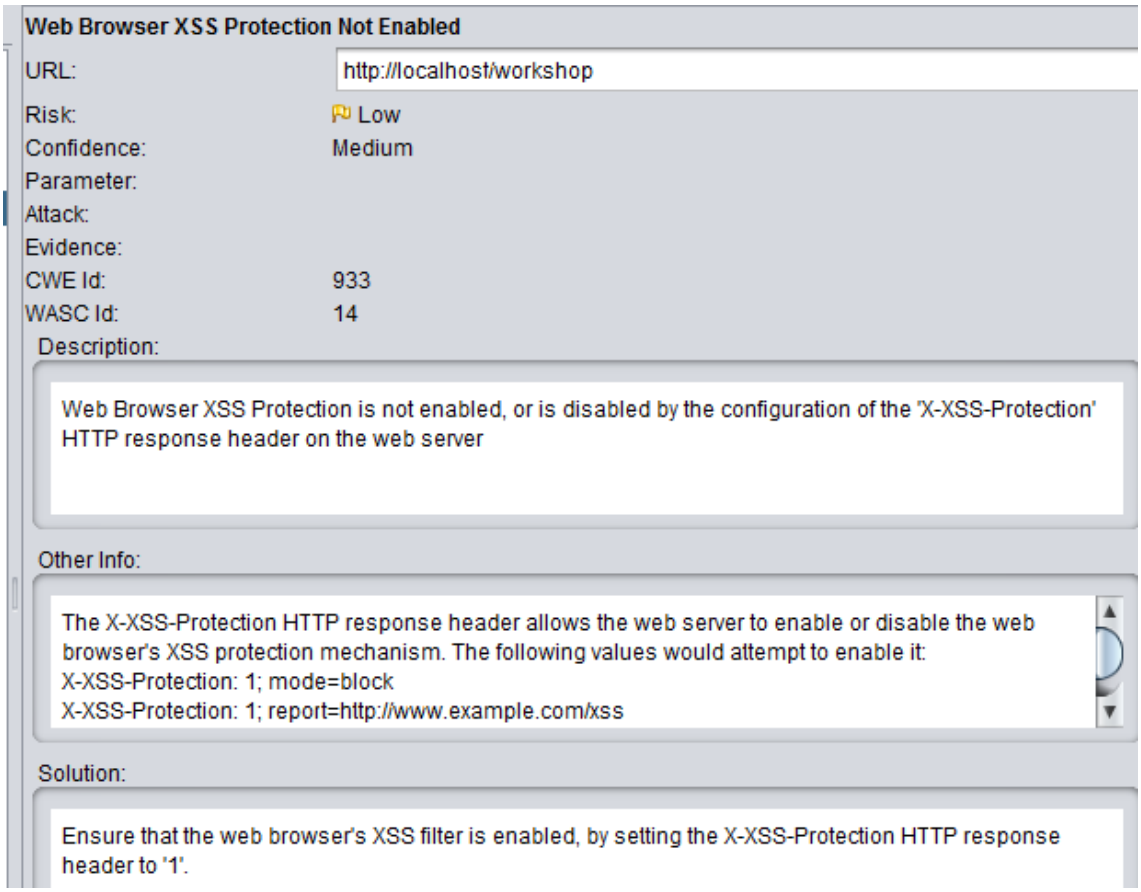

Figure 5. XSS protection error

Solution

This problem was resolved by enabling web browser's XSS filter, setting X-XSS protection in HTTP header.

7 CONCLUSION

This thesis provided a brief introduction to the virtual learning environments and their advantages. It also described data security techniques, databases and web servers and their features along with limitations. Further, it introduced penetration testing tools such as IronWASP, Wireshark, w3af and ZAP.

The main goal of this thesis was to find out the major issues, which could be exploited by the intruders to compromise the system, so that in near future, these issues could be eliminated and help the administrator and programmer to implement useful script to secure the system.

Problems arose in the normal operation of the working space due to the weak points left during the development phase which always give an opportunity for exploitation. To preventthe issues from compromising the working space, research was carried with leading tools in industry, which helped to find solutions to these issues. Five different issues were registered throughout the testing, but three major problems were discussed in detail.The issues in the VLE examined in the thesis were Application error, missing X-frame header , Cookie without HTTPflag, Web browser XSS protection disabled, and missing X-Content-Type header. The solutions to these issues were assessed for their proper execution within a testing environment. The problems that were detected during the testing need to be solved with the solutions outlined in the thesis which will eliminate the weak points.

REFERENCES

[1] Virtual Learning Environment (VLE) or Managed Learning Environment (MLE), Consulted on: 04.05.2015. [online] Available at: http://whatis.techtarget.com/definition/virtual-learning-environment-VLE-or-managed-learning-environment-MLE

[2] The Digital Learning Environment What the Research Tells Us, Consulted on 15.04.2015. [online] Available at: http://www.ssis.edu.vn/uploads/pdf/The_Digital_Learning_Environment.pdf

[3] Selecting a VLE, Consulted on 02.04.2015 [online]. Available at: http://recap.ltd.uk/Web2/vle-select.php

[4] Moving towards the Digital Learning Environment, Consulted on20.04.2015. [online] Available at: http://www.indiana.edu/~rcapub/v19n2/p2.html

[5] Data Classification. Consulted on 09.04.2015. [online] Available : http://www.cmu.edu/iso/governance/guidelines/data-classification.html

[6] Types of Restricted Data, Consulted on 10.05.2015. [online] Available at: http://its.ucsc.edu/security/training/restricted.html

[7] 15 Worst Data Security Breaches of the 21st Century, Consulted on 13.05.2015 [online]. Available at :http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html

[8] Black Hole and Gray Hole, Consulted on 23.04.2015 [online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.206.4786&rep=rep1&type=pdf

[9] Advantages of the IIS Server, Consulted on 03.04.2015 [online]. Available at: http://www.iis.net/learn/get-started/introduction-to-iis/iis-web-server-overview

[10] SQL Injection, Consulted on: 28.04.2015 [online] Available at: https://www.acunetix.com/websitesecurity/SQL-injection/

[11] Database Security Best Practices, Consulted on 15.04.2015. [online] Available at: http://www.applicure.com/blog/database-security-best-practice

[12] Save Your Servers: Three Ways to Reduce the Threat of Viruses, Consulted on 08.05.2015. [online] Available at: www.business2community.com/tech-gadgets/save-servers-three-ways-reduce-threat-viruses-0834245

[13] Types of Security Threats and Their Prevention, Consulted at 08.04.2015 [online]. Available at: http://ijcta.com/documents/volumes/vol3issue2/ijcta2012030240.pdf

[14] Network Intrusion Detection and Prevention Systems, Consulted on 11.04.2015. [online] Available at: http://www.secureworks.com/it_security_services/managed_ids_ips/

[15] Identity Theft Resources Center Breach Report Hits Record High in 2014, Consulted on 03.05.2015. [Online] Available at: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

[16] Weinberg, Paul N. R, Paul. , SQL: The Complete Reference, Third Edition, McGraw-Hill Companies, 1976.

[17] 37 Powerful Penetration Testing Tools, Consulted on 08.04.2015 [online]. Available at: http://www.softwaretestinghelp.com/penetration-testing-tools/