The Comparative Analysis of Online Shopping Information Platform's Security Based on Customer Satisfaction

S M Hasan Mahmud[1], Md Alamgir Kabir [2], Omar M. A. Salem[3], Kazihise Ntikurako Guy Fernand[4]
Department of Software Engineering, Daffodil International University, Bangladesh[1]
International School of Software, Wuhan University, Wuhan, China[2, 3]
Department of Computer Science and Information, Hohai University, Nanjing, China[4]
hasan.swe@daffodilvarsity.edu.bd[1], sagar.iis@whu.edu.cn[2], omarsalem@ci.suez.edu.eg[3], kazihise.guy@gmail.com[4]

***Abstract*—With the massive expansion of Internet and e-commerce technology, Internet platform is providing a lot of services and advantages for online business, especially for online shopping portal. As a result of the Internet, online shopping has expanded in businesses more effectively and online services are collaborating with customers and other associations. For improving online shopping information platform's security, customer satisfaction is one of the most fundamental factors. This paper constructs the measurement of four-dimensional models that are appropriate for measuring customer satisfaction of online shopping information platform's security. This paper also conducts the factor and multiple regression analysis to verify the measurement model. By using questionnaires survey and analysis from the groups of Hohai University students, this research provides suggestions for the development of large online shopping portal and will help to improve customer satisfaction on the security of the online shopping information platforms.**

Keywords—Customer Satisfaction; Platform Security; Online Shopping; Comparative Analysis; Customer Perception

I. INTRODUCTION

In the rapid improvement of the online market, numerous consumers are interested in online marking as a new service mode. In order to fulfill the customer demand, the online shopping portals have developed many online purchasing systems and online payment service systems. In those systems, the user can log in the online portal on the internet to enjoy the online purchasing through the web and mobile application. According to the report of user feedback, technically a well-developed information platform's security is safe enough to ensure customers accounts information for accepting the real challenge of the online shopping payment platform.

The online shopping portal finds few emerging contents: customer satisfaction, service quality, software performance, security, and product tracking. The preventions of the information security problems need to use software-based systems during online purchasing [1]. The behavior of the internet creates opportunities for hackers and other tricksters who would take benefit of companies and vulnerable consumers. Online shopping companies ensure customers information and also secure their personal data when they submit an order or complete a purchase. It may be best for an online business company to install the most up-to-date encryption and secure technology to maintain customers personal data. They also defend the online payment portal from hacking, viruses, malwares and anything that could prevent the online portal from performing perfectly.

China is one of the largest online products sellers in the world. It has some popular online shopping portals such as Alibaba (taobao.com, tmall.com), jd.com etc. These online shopping portals transfer a huge amount of money every day. Last year in October-December 2015, the day average of products selling was 1.2 billion USD by Alibaba (taobao.com, tmall.com) and 98 million USD by Jd.com. Therefore, online shopping portal information security has major responsibilities for online business.

In this paper, by using the satisfaction of domestic and foreign students during online shopping in Alibaba (taobao.com, tmall.com), We have designed a four-dimensional model with eight sub-factors, based on the influence factors of online shopping information platform's security. The result of the empirical analysis of this paper is able to give an idea about how to improve the quality of the online shopping portal information platform's security, from the customer's point of view. The increase of customer satisfaction improves the quality of the online portals, which increases the competitiveness of rapid development in online network market correspondingly.

The rest of the paper is organized as follows: Section II contains the related work; Section III explains the research model and hypothesis; Section IV presents the empirical analysis and finally section V concludes the paper.

II. RELATED WORK

In the area of online shopping customer satisfaction part, many domestic and foreigner researchers proposed several approaches. Oliver (1980) defined that customer satisfaction is the realization caused by a customer after using a product or service. Customer perception service quality is the central of assessment, while customer's satisfaction is connected with individual transaction [2]. Ma (2012) purposed a research

An Analytical and Comparative Study of Software Usability Quality Factors

Usability Model in Software Engineering Literature

Md Alamgir Kabir and Muaan Ur Rehman
International School of Software
Wuhan University, Wuhan China
{sagar.iis, rahmani}@whu.edu.cn

Shariful Islam Majumdar
Department of Multimedia and Creative Technology
Daffodil International University, Dhaka Bangladesh
sharif.mct@daffodilvarsity.edu.bd

***Abstract*— The demand of quality software is increasing day by day. In the recent economic world, software is used for fast business and quality software is also necessary for satisfying the customer demands. So for assuring and improving quality, it is necessary to ensure quality attributes such as usability, efficiency, learnability and many more. Among of them, usability is the key quality attribute of any kind of software. With the same time, evaluation of usability is also necessary for improving the quality of the software. There have many quality models emphasized usability as a major quality attribute. Last few years researchers have developed many quality models described usability as a sub quality factor. Now it is time to develop a usability model that will contain major quality attributes of the current complex business software. In this paper, we have analyzed ten famous quality models for developing a usability model which satisfy the demand of current business software. We also have showed the analytical comparison among the famous ten quality models for usability factor. At last, we have proposed an integrated improved usability model for assuring software quality.**

Keywords- Software Quality; Quality Model; Usability; Usability Evaluation

I. INTRODUCTION

In the competitive economic market, the demand of quality software is rising rapidly. But at the same time, the rejection of software is also increasing because of customer demand and quality software. So the question is, what is quality? Quality means the standard of something as measured against other things of a similar kind; the degree of excellence of something. That means quality is a term which can be measured of something that is standard. So software quality means the software meets the user requirements. For this user requirements are the first para meter for measuring the software quality. When user will satisfy the software that means the software meets the requirements. Then we can say that the software is quality system. According to Software and Systems Engineering Vocabulary Data Base, degree to which a system, component, or process meets specified requirements [1].

For measuring and assuring quality, last few years researcher have developed many quality models. Quality model consists of quality factors such as usability, learnability and efficiency. Among of them, usability is the major quality factor because it major impacts on software acceptance.

Many software engineers, industry experts and researchers define the usability in many ways. According to Ankita Madan et al. usability is a product attribute that influences the quality of a software system [2]. The Institute of Electrical and Electronics Engineers define as "the ease with which a user can learn to operate, prepare inputs for and interpret outputs of a system or a component" [3].

There are many quality models emphasized usability as a main quality factor. The developed model also divided usability as many factors. In this paper, we have analyzed famous ten software quality models for selecting usability quality factors. Here we also showed analytical comparison of usability quality factors. We also proposed an improved usability model based on the analysis.

This paper is structured as follows. Section II provides an overview of ten famous quality model. Section III discusses the comparison of usability factor. Section IV represents the proposed usability model. Finally, Section V concludes this paper and gives an overview of our future work.

II. OVERVIEW OF TEN QUALITY MODEL FOR USABILITY FACTORS

This section presents quality models and discusses the usability factors of the famous models. These models are McCall's, Boehm's, Brian Shackel, FURPS, Jakob Nielson Quality Model, Software Usability Measurement Inventory (SUMI) Quality Model, ISO 9241 – 11 Quality Model, ISO 9126 Quality Model, Quality in Use Integrated Measurement (QUIM) and Software Engineering Methodologies (SEM) Quality Model.

McCall's Quality Model (1977) has three perspectives. These are product revision, production transition and product operations [4]. But product operations have five factors. Among of them, usability is the key issue of product operations and usability has three factors: operability, training and communicativeness.

Boehm's Quality Model (1978) have three types of characteristics: high level characteristics, intermediate level

978-1-4673-9904-3/16/$31.00 ©2016 IEEE

SQLi Penetration Testing of Financial Web Applications: Investigation of Bangladesh Region

Tanjila Farah
Dept. of ECE
North South University
Dhaka, Bangladesh
Email: tanjila.farah@northsouth.edu

Delwar Alam, Md. Alamgir Kabir, and Touhid Bhuiyan
Dept. of Software Engineering
Daffodil International University
Dhaka, Bangladesh
delwaralam@gmail.com, alamgir.swe@diu.edu.bd, t.bhuiyan@daffodilvarsity.edu.bd

***Abstract*—Business critical web applications are the most popular services provided to the client by the financial sector. These applications are bringing handsome revenue for the financial industry every year. These services are also a frequent target of attackers. Poor coding practice leads applications to vulnerability that are exploited by attackers. Information and privileges such as access to databases, admin authorization, and access to data could be retrieved through exploitation. Services provided through web applications make the exploitation easier as these could be accessed from anywhere around the world. Web based financial services are comparatively new concept in Bangladesh. Thus the security aspects of these applications are less explored. This paper represents an analysis of few basic security issues of the financial web applications of Bangladesh. It focuses on structured query language injection (SQLi) vulnerability. It presents a manual black box penetration testing approach to test the financial web applications. Same steps are used for testing all the web applications in the dataset. A vulnerability analysis of the findings collected during the penetration testing is also presented in the paper.**

Keywords – Financial web application; penetration testing; black box testing; SQLi.

I. INTRODUCTION

Web applications are the programs accessed through Internet connection. These applications use HTTP as their primary communication protocol and a back-end database to provide real time service to the users. The services provided by the web applications include: education, health care, news, financial transaction and more [1]. The financial web applications has become an essential element of the enterprise business activities. As popularity increases these services have also become a target of various cyber threats [7]. As per studies financial web services suffer the most security breaches every year [4]. There are various tools and organizations for checking the security level of financial service applications [5], [6]. Designing of financial application follows various regulatory requirements and they are implemented using secure coding [8], [9]. Even then the security of these applications is breached and confidential data are stolen every day. The key aspects of these violations are the vulnerabilities present in the web applications. These vulnerabilities or threats include: invalidated input fields, structured query language injection (SQLi), cookie poisoning cross site scripting, parameter tempering etc [4]. Vulnerability assessment and penetration testing are used for prevention of attacks on application services [2]. Vulnerability assessment is the gateway through which threats are discovered. Penetration testing is a security evaluation process that simulates real attack on the web applications to discover the vulnerabilities. The assessment is done based on the comparison of actual and expected behavior of the web applications [3]. There are various methods of penetration testing. For successful testing, following a methodology is necessary [1]. Although the names and sequence of the methodology of testing differ, the underlying processes are the same for all methods [9]. The goal in this paper is to perform vulnerability assessment and penetration testing on the financial websites of Bangladesh. The SQLi vulnerability is focused in this paper. Black-box penetration testing approach is used for testing purpose [4]. The paper is organized as follow. The methodology of the testing is discussed in section 2. Analysis of the testing code is presented in section 3. In section 4 the results of the test is analyzed. Conclusions are drawn in section 5.

II. METHODOLOGY OF PENETRATION TESTING

Penetration testing methodologies are systematic approaches of test techniques to corroborate the existence of vulnerabilities. It focuses on locating and targeting exploitable defects in the design and implementation of a web application. Penetration testing could be performed manually or by using automatic tools [3]. Successful penetration testing depends on the methodology. Various groups follow various methodologies for penetration testing. The existing testing methodologies include 4 to 7 steps. Though the names of these steps are different in various methodologies the functions are the same [1]. NIST penetration testing methodology is used in this research [3]. This methodology includes four phases: planning, discovery, attack, and reporting. These phases are further subdivided to make the steps of testing method accurate as shown in Fig 1.

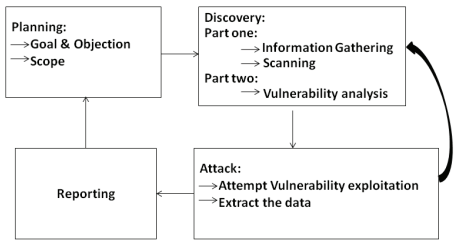

Figure. 1. Penetration testing steps

SQLi Vulnerabilty in Education Sector Websites of Bangladesh

Delwar Alam
Dept. of Software Engineering, Daffodil International University, Dhaka, Bangladesh
delwaralam@gmail.com

Touhid Bhuiyan
Dept. of Software Engineering, Daffodil International University, Dhaka, Bangladesh
t.bhuiyan@diu.edu.bd

Md. Alamgir Kabir
International School of Software, Wuhan University, China
sagar.whu@outlook.com

Tanjila Farah
Dept. of ECE, North South University, Dhaka, Bangladesh
tanjila.farah@northsouth.edu

Abstract— Bangladesh has announced every Government & Non –Government school and colleges must website. The websites have to include all data and information every school and colleges. The goal of this initiative is to ensure equal quality of education and to provide education to the remote areas of the country. Though is a very new concept yet an appreciable number of institutes have already started shifting their systems online. While this advancement is commendable yet there are drawbacks such as security risks of these websites and the data in them. One of the easiest yet treacherous security risks of website is SQLi. This paper focuses on various types of SQLi vulnerabilities such as: normal, error based double query, and blind injection techniques and their aggression on the educational websites of Bangladesh. Manual penetration testing with black box approach has been implemented in number of web applications to check the vulnerabilities. The data found has been analyzed to draw statistical conclusion of the present condition of the educational websites of Bangladesh.

Keywords—Blind injection, Error based injection, Double query, SQLi.

I. INTRODUCTION

Educational websites have been proven most efficient by providing easy access to education in any part of the world. Quality education is now a day is not bound to a country or place. Anyone with an internet connection can go across the world and study by sitting at home. Though the use of web applications is a very new concept Bangladesh government's initiative has been highly appreciated adopted in all educations sectors. At present in our country has estimated 0.13 million school. After Bangladesh governments announcement in July 2015 about 30 thousand schools and colleges have already registered for website domain [12]. Among this 30 thousand a large number of school and college have already lunched their websites. Website security and maintenance are also a new sector. Carelessness and poor coding practice of website developers make web applications vulnerable to various cyber attacks. Consequence of these attacks may vary from false news publication to changing exam results. However the security issues of educational websites are barely addressed as of now. The website owners are not even aware of the threats. The types of vulnerability also depend on which types of website development platform are used in certain areas. In Bangladesh region the most used website development platform php with MySQL database. One of the major vulnerability of these platforms is various Structured Query Language injection (SQLi) attack [1]. There are various types of SQLi attack such as: normal SQLi, error based SQLi, double query and blind injection [3]. All these attacks result in retrieving user sensitive information without authorized permission. This paper presents an assessment and analysis of three major SQLi technique implemented on the educational websites of Bangladesh. The data is analyzed based on type of SQLi vulnerability, level of vulnerability and the type of sensitive information's collected through testing.

The paper is organized as follow. In section 2 SQLi and types of SQLi are explained. In section 3 data analysis is presented. And then we conclude in section 4.

II. SQLI AND TYPES OF SQLI

SQL is the language for communicating with database. Users write the URL of the website in their browser. The database doesn't understand this language [1]. This URL is converted to SQL query by the web server and sent to the database server as shown in Figure 1. The database reads and understands the query. It then matches the requested item with the items saved in the database and returns the matched item.

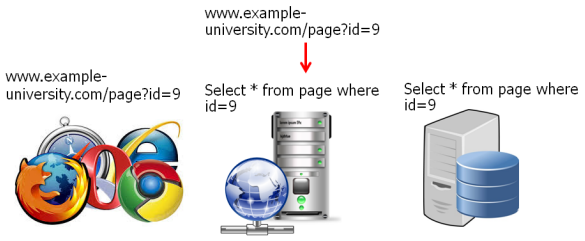

Figure 1. URL to query conversion

When the URL input is crafted to return unauthorized output, The query is claaed SQLi. The crafted input is converted into query in the same process shown in Figure 1. This type of Vulnerability occurs when the user input parameters are not verified before forming the query.There are various types of

Proc. of The Third Intl. Conf. on Advances in Computing, Electronics and Communication - ACEC 2015

ISBN: 978-1-63248-064-4 doi: 10.15224/ 978-1-63248-064-4-23

Exploring the SQL injection vulnerabilities of .bd domain web applications

Delwar Alam, Tanjila Farah, Md. Alamgir Kabir

***Abstract*—Web applications have been proven most efficient by providing easy access to services such as online education, banking, reservation, shopping, resources, and information sharing. Though the use of web applications is a comparatively new concept, various government and private organizations of Bangladesh have started getting accustomed to it. Bangladesh government has also taken initiative to support web based services and ensure their security and reliability. Most of the web applications of Bangladesh are registered under .bd domain. The global accessibility and sensitivity of the information's of web applications make them a target for web attackers. However the security issues of the .bd domain web applications are not addressed. No through study has been done so far on the existing vulnerabilities of these web applications. Hence the web applications are vulnerable to basic attack such as Structured Query Language injection (SQLi). This paper presents an evaluation of existing User input based SQLi vulnerability of web applications of .bd domain using black box penetration testing approach. The tests are performed manually. The data collected are analyzed to provide a guideline for website administrators.**

Keywords—*component, formatting, style, styling, insert* (key words)

I. Introduction

Web applications provide friendly interface and easy accessibility to the internet users. Various companies have launched web applications of their products to make their merchandises available worldwide [1]. With this increasing popularity, ensuring the security of these applications are also becoming a major concern. Web applications are dynamic as they are associated with back-end database and allow users to store and retrieve real time data [2]. However this also makes the database accessible by the intruders who intend to access database to retrieve unauthorized sensitive information and perform malicious activity through them. This results in security violations including identity theft, fraud, and control and corruption of web services [1], [9]. Database oriented web application are vulnerable due to design flaws such as: lack of input sanitization, unnecessary construction of dynamic queries, and unnecessary access to information [3]. Attackers inject unauthorized input or malicious code by manipulating design flaws to get unrestricted access of the web application database and thus the user data [4]. There are various exploitation techniques available. Structure query language Injection (SQLi) and Cross site scripting (XSS) are two of the most used exploitation [5]. Over the past few years there has been plenty of research in these fields of web application security, their types and vulnerabilities [[6], [8]. There are various sub types of SQLi and XSS [7]. In this paper we present an assessment and analysis of User-input based SQLi technique implemented on the web applications of .bd domain. We have considered two subtypes of SQLi: POST() based and GET() based methods for this research [10]. For analysis purpose the data is divided based on GET() and POST() method. This paper is organized as follow, we start by describing SQL, various SQLi and GET() and POST() based SQLi. In section 3 we explain the research methodologies. In section 4 we describe the steps of SQLi we used during the research. Section 5 we discuss our finding of the research. And then we conclude in section 6.

Delwar Alam
Daffodil International University
Bangladesh

Tanjila Farah
North South University
Bangladesh

Md. Alamgir Kabir
Daffodil International University
Bangladesh

II. Background

Web applications operate by user writing the URL/address of the application in the browser. The browser carry the URL to the web server connected to the database. Between server and database is firewall that blocks any unauthorized requests to get connected to the database as shown in Figure 1. Most of the requests coming through browsers are allowed to bypass the firewall. These requests are known as http request. Once the browser provided request passes the first firewall the web servers use the request to form a SQL query. This query passes the second firewall to reach the database and retrieve information requested by the user. The same process is used by the adversaries to inject malicious input to the database and retrieve unauthorized data.

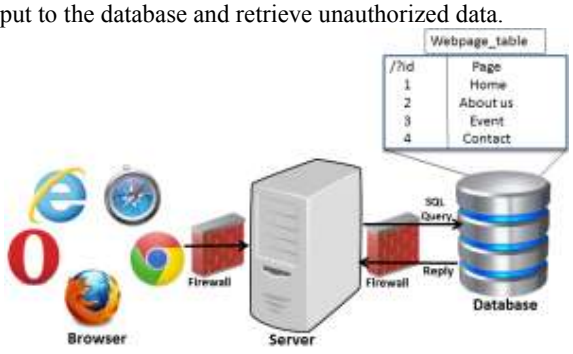

Figure 1. Connect to the database to retrieve data

2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)
19-20 December 2015, BUET, Dhaka, Bangladesh

Investigation of Bangladesh Region Based Web Applications: A Case Study of 64 Based, Local, and Global SQLi Vulnerability

Tanjila Farah
Dept. of ECE
North South University
Dhaka, Bangladesh
Email: tanjila.farah@northsouth.edu,

Delwar Alam, Md. Nadir Bin Ali
Dept. of Software Engineering
Daffodil International University
Dhaka, Bangladesh
delwaralam@gmail.com, it@daffodilvarsity.edu.bd,

Md. Alamgir Kabir
International School of Software,
Wuhan University,
China
sagar.whu@outlook.com

***Abstract*—Government and private organizations of Bangladesh have started getting adopted to various web applications due to the easy accessibility. Services provided by web applications include online education, banking, reservation, shopping, resources, and information sharing. However the awareness of web application security has not been developed yet. No through study has been done on the existing vulnerabilities of these web applications of Bangladesh. This paper presents an investigation of the current vulnerabilities in the web applications of Bangladesh. This paper focuses in various web application firewall available in the web applications of Bangladesh and the SQLi techniques to evade these firewalls. The data collected are analyzed to provide a guideline for web application developers and administrators of Bangladesh.**

Index Terms – 64based SQLi, Local SQLi, Global SQLi, web applications, injection vulnerability.

I. Introduction

Websites and web application security is becoming a new concern in Bangladesh. Friendly interface of web applications are increasing the their popularity. Initially Bangladesh governments goal was to get the people accustomed to the use of website and web applications. The government has been very successful in this goal. Most of the government institutes has launched online services to the people. The popularity and usage of these services has made them a target of attackers. Various studies has been done on the current conditions of the web based services of Bangladesh [1], [2], [3]. Yet this studies are not enough. These papers focused on basic structured query language injection (SQLi) techniques and their vulnerabilities in websites of Bangladesh [2]. Structured Query language (SQL) is used to retrieve data from database [6]. Intruders violate the relation between application and database by inserting unauthorized data and thus prompting the database to act out maliciously [5]. This process of inserting malicious and unchecked input in database is known SQL injection (SQLi) attack [7]. Another attack that follows the similar process is cross site scripting (XSS). SQLi and XSS are a potential threat to all database driven web applications [11], [8]. Recent studies also focused on various web application firewalls used in the website to prevent SQLi attacks [1]. Various techniques and firewall have been introduced to prevent SQLi and XSS vulnerabilities [9], [10]. Studies show WAF's are not enough and breakable using various techniques. This paper explores the WAF based SQLi vulnerabilities exist in the web applications of Bangladesh. It presents an analysis 64based SQLi, Local and global variable SQLi techniques. 64based SQLi is a WAF evasion technique used in web application that has 64 based URL encoding. Local and global variables are SQLi are two properties of MySQL database based websites. This paper is organized as follow, we start by describing SQL, WAF and WAF evasion techniques. In section 3 we explain our research methodology. In section 4 we discuss our finding through this research. And then we conclude in section 6.

II. Background

Web applications communicate by users writing the URL of the application in the browser. This URL is then processed by web server connected to the database through a firewall. Firewalls in server usually blocks any unauthorized access to the database. The firewall is known as web application firewall (WAF). The web servers use the request to form a SQL query. The same process is used by the adversaries to inject malicious input to the database and retrieve unauthorized data.

A. SQL

Structured Query Language is a programming language used to communicate and control databases connected to web applications. Once the users request for a web application reaches the web application server, it dynamically generates a SQL query based on the users input. For example, consider a web application, www.xyz-example.com shown in Figure 1. The URL has two parts: the web application name and the value. The value is used to retrieve a specific page from that web application.

B. WAF

Web application firewall (WAF) is a security measure taken by web developers to protect the websites/web applications from unauthorized inputs from the users end. WAF works by validating the inputs provided by the users. WAF is placed between the web application and web application server. User to web server request and response syntax and inputs are very specific. For example the pages of a website are usually saved in the database server with an id or a name. When

978-1-4673-8786-6/15/$31.00 ©2015 IEEE

2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic

A Case Study of SQL Injection Vulnerabilities Assessment of .bd Domain Web Applications

Delwar Alam, Md. Alamgir Kabir, and Touhid Bhuiyan
Dept. of Software Engineering
Daffodil International University
Dhaka, Bangladesh
Email: delwaralam@gmail.com, alamgir.swe@diu.edu.bd, t.bhuiyan@daffodilvarsity.edu.bd

Tanjila Farah
Dept. of ECE
North South University
Dhaka, Bangladesh
tanjila.farah@northsouth.edu

***Abstract*—Web applications or services play an important role in present day to day life. They have impact on the development of both individual and a country. Easy access to services such as online education, banking, reservation, shopping, resources, and information sharing have been proven most efficient for every day life. Various government and private organizations of Bangladesh have started to use web services to support clients. Most of the web applications of Bangladesh is registered with *.bd* domain and developed using content management system (CMS), various scripting language and SQL or MySQL database. Web applications are popular target for web attackers. However the security issues of the *.bd* domin web applications are not looked appropriately upon as of yet. One of the most attacked vulnerability of the database driven web applications is SQL injection or SQLi. SQLi through URL and user-input field is extremely high risk in current web based applications. Restricting user access to URL and user input field defies the purpose of web applications. However, the un-restricted user access exposes the vulnerable fields to web attacks. To prevent these exploitation's it is essential to have knowledge of the vulnerabilities adversaries uses to exploit the web applications. This paper presents an evaluation and analysis of SQLi vulnerabilities present in the existing web applications of *.bd* domain using black box penetration testing approach. User input based SQLi has been used for evaluation.**

Index Terms – SQLi, web applications, vulnerability, get and post based SQLi.

I. Introduction

Web applications provide friendly interface and any time easy accessibility. As the popularity of web applications is increasing. it is bringing billions of dollars in annual revenue [1]. Various government and private organizations have started to launch various web application services in Bangladesh such as: financial transaction and information sharing services. Though launching a web application for each service has become a trend, the security aspects are not considered as seriously. This places the companies and the users of the applications in serious security risks. Security issues arise based on the platform and structure of the web applications. Web applications associate with back-end database for storing and retrieving real time data. Users provide input though web application to retrieve output from database. Structured Query language (SQL) is used to retrieve data from database [3]. Intruders violate the relation between application and database by inserting unauthorized data and thus prompting the database to act out maliciously [2]. This process of inserting malicious and unchecked input in database is known SQL injection (SQLi) attack [4]. Another attack that follows the similar process is cross site scripting (XSS). SQLi and XSS are a potential threat to all database driven web applications [8], [5]. Over the past few years there has been plenty of research going on in this field of web application security, their types and their vulnerabilities. Various techniques and firewall have been introduced to prevent SQLi and XSS vulnerabilities [6], [7]. Yet these vulnerabilities remain threat to web applications. This paper explores the SQLi vulnerabilities exist in the web applications of Bangladesh. It presents an analysis of user-input based SQLi technique implemented on the web applications. The black box approach is used for testing purpose. Get and post based SQLi techniques has been considered for analysis purpose [8]. This paper is organized as follow, we start by describing SQL, various SQLi and get and post based SQLi. In section 3 we explain our research methodology. In section 4 we describe the steps of SQLi we used during the research. Section 5 we discuss our finding through this research. And then we conclude in section 6.

II. Background

Web applications are accessed by user writing the URL/address of the application in the browser. The browser receives the URL and proceed them to the web server connected to the browser through firewall. Web server is also connected to the database through a firewall. Firewalls block any unauthorized requests to get connected to the database. To provide a user friendly interface to web services, most of the requests coming through browsers are allowed to pass the firewall. Once the browser provided request reaches the web servers, the request is used to form a SQL query. This query then passes the firewall between web and database server to reach the database and retrieve information requested by the user. The adversaries to SQL request to inject malicious input to the database and retrieve unauthorized data. The connections between browser, web server, and database server are shown in Figure 1.

A. SQL

Structured Query Language is a programming language used to communicate and control databases connected to web application. Once the users request for a web page/web application reaches the web application server, it dynamically forms a SQL query based on the users input. For example,

978-1-4673-8499-5/15 $31.00 © 2015 IEEE
DOI 10.1109/CyberSec.2015.23

National Conference on Communication and Information Security (NCCIS 2012)
Daffodil International University, Dhaka, Bangladesh, 31 March 2012.

Life Cycle Implementation of an Android Application for Self-Communication with Increasing Efficiency, Storage Space and High Performance

Md. Alamgir Kabir, A.J.M. Imtiajur Rahman and Md. Ismail Jabiullah
Department of Software Engineering,
Daffodil International University, Dhaka, Bangladesh
Email: sagaryho@yahoo.com

Abstract— **Android is a Linux-based platform for mobile devices such as smartphones and tablet computers. It is developed by the Open Handset Alliance led by Google. Android delivers a complete set of software for mobile devices: an operating system, middleware and key mobile applications. In this paper, some of the phases of the system development life cycle have been implemented on android application and analyze the result of testing for efficiency, storage space and performance of the application.**

Keywords: smartphone, Linux Kernel, SDLC, Life Cycle and Android..

I. INTRODUCTION

Android is an operating system that includes middleware and key applications. Android Inc. was founded in Palo Alto of California, U.S. by Andy Rubin, Rich miner, Nick sears and Chris White in 2003 [2]. Later Android Inc. was acquired by Google in 2005. After original release there have been number of updates in the original version of Android. There has been big barrier of broad scope of embedded devices software especially if we talk about the operating systems of embedded devices. Still abundantly used embedded device like mobile phones are still living on proprietary operating systems, to work on those systems developers have to pay heavy price to purchase development environment and build-linker-debugging tools. This leads to slow development in overall mobile development field, since lots of homebrew developers unable to put their research and development knowledge.

This barrier to application development began to crumble in November of 2007 when Google, under the Open Handset Alliance, released Android [1]. The Open Handset Alliance is a group of hardware and software developers, including Google, NTT DoCoMo, Sprint Nextel, and HTC, whose goal is to create a more open cell phone environment. The first product to be released under the alliance is the mobile device operating system, Android. Android is what's known as open source and, to a large degree, that means that its inner workings and machinations are free to for the public to access, view and even tinker with. Android will ship with a set of core applications including an email client, SMS program, calendar, maps, browser, contacts, and others. All applications are written using the Java programming language. Android was built to be truly open. For example, an application can call upon any of the phone's core functionality such as making calls, sending text messages, or using the camera, allowing developers to create richer and more cohesive experiences for users. Android is built on the open Linux Kernel. Furthermore, it utilizes a custom virtual machine that was designed to optimize memory and hardware resources in a mobile environment. Android provides access to a wide range of useful libraries and tools that can be used to build rich applications. For example, Android enables developers to obtain the location of the device, and allows devices to communicate with one another enabling rich peer–to–peer social applications. In this paper, life cycle phase of the system development life cycle (SDLC) has been implemented. This approach imposes better efficiency, increases performances in storage capacity and show high performances in the self communication environment.

II. CONVENTIONAL APPROACH [3]

Android allows developers to write managed code in the Java language, controlling the device via Google-developed Java libraries. Applications written in C and other languages can be compiled to ARM native code and run, but this development path isn't officially supported by Google. Android is available as open source.

A. Application Lifecycle

In Android, the applications are run as a separate Linux process. So the application lifecycle is closely related to the process lifecycle. The application process lifecycle is handled by the system depending on the current system memory state (Fig. 1). In case of low memory, the Android

International Journal of Smart Home
Vol. 10, No. 7 (2016), pp. 269-282
http://dx.doi.org/10.14257/ijsh.2016.10.7.27

An Improved Usability Evaluation Model for Point-of-Sale Systems

Md Alamgir Kabir, Bo Han

International School of Software, Wuhan University, Wuhan, 430079, China
Corresponding Author: Bo Han, Email: bhan@whu.edu.cn

Abstract

Point-of-sale (POS) systems are popular in developing countries because they provide fast and convenient ways of transactions for business. These systems contain vital tasks such as online transactions, ecommerce facilities, security, taxes, various management reports and others. Thereby, it is important to ensure their software quality and grantee the effective usages of business functions. Among multiple software quality attributes, usability is highlighted for POS software since the user interfaces are directly linked to cashiers' behaviors, customers' satisfactions and market profits. However, the usability evaluation of POS systems is not easy since they are generally featured with multi-functions, multiple configurations and complex interfaces. Many available quality models have failed to evaluate the usability of POS systems because any of them just cover partial view of usability. In this paper, we investigated ten well-known quality models and extracted the usability related factors from each of these models. By integrating these factors together, we proposed an improved usability evaluation model with a comprehensive view of usability for POS systems. Following the model, we designed usability scenarios for each factor and thus provided the corresponding questionnaires. A case study of evaluating a POS system in Bangladesh has demonstrated that the proposed model can provide a comprehensive evaluation of POS from 12 usability factors. Also, different demands from different type of customers are also be revealed by the model.

Keywords*: Usability Models, Point-of-Sale, Quality Model, Usability Evaluation*

1. Introduction

Nowadays, Point of Sale (POS) systems are popular in developing countries because they provide fast and convenient ways of transactions for business. These systems contain vital tasks such as online transactions, ecommerce facilities, security, taxes, various management reports and many more [1]. Therefore, with large volume of customers in supermarkets and the growing competitive business environment in developing countries, ensuring the software quality becomes very important for them.

Among multiple software quality attributes, usability is highlighted for POS software since the user interfaces are directly linked to cashiers' behaviors, customers' satisfactions and market profits [2, 4-6]. A friendly user interface will provide effective helps to cashiers and faster checkout of customers, decreased in-store customer traffic, increased management reporting capacity, and also access to more consumers [3, 31]. According to Len Bass *et al.*[8], usability depends that how easy a system accomplishes users' tasks and to what extend users support system functions. According to Nielsen [9], usability is a quality attribute that assesses how easy user interfaces are to use. Usability depends on the match between a software product and its users under the particular constraints of the environment and tasks being performed with the product [7 -22]. Accordingly, usability of POS systems examines the interaction between users and POS software [10-11].

ISSN: 1975-4094 IJSH

J. Bangladesh Electron. 13 (1-2); 13-21, 2013

A Survey on Process Oriented User Security Questions Based Approaches in Requirements Engineering

Md. Alamgir Kabir[1], Sydul Islam Khan[2] and Md. Ismail Jabiullah[3]

[1]*Department of Software Engineering, Daffodil International University*
[2]*Department of Computer Science and Engineering, Daffodil International University*
[3]*Department of Computer Science and Engineering, Hamdard University Bangladesh*

E-mail: sagarho@yahoo.com, ksonju@yahoo.com, mijjabi@yahoo.com, mij1996@gmail.com

Abstract

Secure software development is the new attention of current world in recent days. Security is the key issue for assuring the quality full software. Since, security is one the non-functional requirement most of the times it is ignored in the requirements phase. But, it is possible to reduce software development cost and time to identify user security requirements in the early stage of the software development process. IT security must apply to ensure the reliable system and protect assets of the business organization. In this scene, the main deal is to present the user security requirements combining with user functional requirements which are collected form requirement phase in Software Development Life Cycle (SDLC). Secure Software Development Life Cycle (SSDLC) start from security requirements. If we can elicit user security requirements and present these requirements in requirements phase which are user process oriented then secure software develop will be ensure from the very beginning. In Industry and academic, there are several methods to elicit and analyze the process oriented user security requirements, but few methods are efficient in identifying and presenting the user security requirements. This paper reflects the current research on process oriented user security question based approaches in requirements engineering phase. We try to identify the research trend, based on related published work.

Keywords: Security Requirements, Requirements Phase, Secure Software Development Life Cycle, Security Requirements Model, User Security Questions Based Approaches

1. INTRODUCTION

In the competitive economic market, the demand of secured and reliable system is increasing day by day. A successful software development is possible by considering equally both functional and non-functional requirements. For this issue, nonfunctional requirements are much important like functional requirements. There are few generic nonfunctional requirements for a system like auditability, extensibility, maintainability, performance, portability, reliability, security, testability, usability and etc. among them security is very vital issue for system development. If we want to develop a reliable and secure system, we have to more concern about security before developing the system that means as early stage in software development life cycle. And this will be requirements stage. In requirements stage, generally we collect user functional requirements. But if we collect user security requirements with user functional requirements then secure software development will be possible with less effort and less cost. Because if user security requirements is arranged after some development from users or stakeholders then it is more difficult, costly and matter of time to combine with user functional requirements with the product or module.

In real sense, user security requirements mean the security requirements for a specific requirements or function. That means for a login system, user name or password is necessary for a successful login. But if the users or stakeholders enter wrong user name or password simultaneously and continuously then some effect will be occurred for security purpose. But the users or stakeholders can enter user name and password two or three times which is specified

American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-12, pp-360-366
www.ajer.org

Research Paper Open Access

A Survey on Security Requirements Elicitation and Presentation in Requirements Engineering Phase

Md. Alamgir Kabir, Md. Mijanur Rahman
[1, 2] *(Department of Software Engineering, Daffodil International University, Bangladesh)*

Abstract: - Secure software development is the new attention of current world in recent days. Security is the key issue for assuring the quality full software. Since, security is one the non-functional requirement most of the times it is ignored in the requirements phase. But, it is possible to reduce software development cost and time to identify user security requirement in the early stage of the software development process. IT security must apply to ensure the reliable system and protect assets of the business organization. In this scene, the main deal is to present the user security requirements combining with user functional requirements which are collected form requirement phase in Software Development Life Cycle (SDLC). Secure Software Development Life Cycle (SSDLC) start from security requirements. If we can elicit user security requirements and present these requirements in requirements phase then secure software develop will be ensure from the very beginning. In industry and academic, there are several methods to elicit and analyze the user security requirements, but few methods are efficient for identifying and presenting the user security requirements. This paper reflects the current research on software user security requirements elicitation techniques in requirements engineering phase. We try to identify the research trend, based on related published work.

Keywords: - *Requirements Phase, Security Requirements Engineering, Secure Software Development Life Cycle, Security Requirements Model, Security Requirements*

I. INTRODUCTION

In the competitive economic market, the demand of secured and reliable system is increasing day by day. A successful software development is possible by considering equally both functional and nonfunctional requirements. For this issue, nonfunctional requirements are much important like functional requirements. There are few generic nonfunctional requirements for a system like auditability, extensibility, maintainability, performance, portability, reliability, security, testability, usability and etc. among them security is very vital issue for system development. If we want to develop a reliable and secure system, we have to more concern about security before developing the system that means as early stage in software development life cycle. And this will be requirements stage. In requirements stage, generally we collect user functional requirements. But if we collect user security requirements with user functional requirements then secure software development will be possible with less effort and less cost. Because if user security requirements is arranged after some development from users or stakeholders then it is more difficult, costly and matter of time to combine with user functional requirements with the product or module.

In real sense, user security requirements means the security requirements for a specific requirements or function. That means for a login system, user name or password is necessary for a successful login. But if the users or stakeholders enter wrong user name or password simultaneously and continuously then some effect will be occurred for security purpose. But the users or stakeholders can enter user name and password two or three times which is specified in requirement stage for specific requirement or function then this type of security purpose is achieved from early stage with less effort, time and cost.

Beyond this introduction on the background details, rest of the paper is organized as follows: In Section II, Security Requirements (SR) in Software Development Process is briefly reported, In Section III, Security Requirements Engineering is briefly reported, whereas in Section IV, we present Security Requirements Elicitation and Presentation Model is briefly reported. Finally, Conclusion is drawn in Section V.

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 75-82
www.iosrjournals.org

Model for Identifying the Security of a System: A Case Study of Point Of Sale System

Md. Alamgir Kabir Sagar[1], Md. Mijanur Rahman[2] and Md. Ismail Jabiullah[3]
[1,2] *Department of Software Engineering, Daffodil International University, Dhanmondi, Dhaka, Bangladesh.*
[3] *Professor and Head, Department of Computer Science and Engineering, Hamdard University Bangladesh, New Town, Sonargaon, Narayangonj, Bangladesh,*

Abstract: *In the competitive economic market the demand of secured and reliable system is increasing day by day. A successful system development is possible by consider equally both functional and nonfunctional requirement. But practically nonfunctional requirements are not identifying as like functional requirement. There are few generic requirements for a system like auditability, extensibility, maintainability, performance, portability, reliability, security, testability, usability and etc. among them security is very vital issue for system development. The security of web based application is vulnerable now a days. For this reason the importance of web based application security is growing over the time. Very often the system fails because of without incorporating the appropriate security specific-process. Our proposed model elicits the system security in a systematic way during requirement analysis phase. Using use case and questionnaires table our model elicits the security requirements of a system. We use Point of Sale System as a case study to identify its security.*

Keywords- *Identify Security, Web Application, Security Model, Functional requirement, Non Functional Requirement*

I. Introduction

The Internet, and in particular the World Wide Web, have become one of the most common communication mediums in the World [1]. Millions of users connect every day to different web-based applications to search for information, exchange messages, interact with each other, conduct business, pay taxes, perform financial operations and many more [1]. For these, web based application is increasing day by day and vulnerabilities of web based application is increasing simultaneously. For securing web based application, we have to secure the network, secure the host and secure the application in Fig. 1 [2]. In this paper, we proposed a model for building secure web based application which is related in application not in host and network. For building a secure application, nonfunctional requirements are necessary along with functional requirements. The term security which is types of nonfunctional requirements. So only functional requirements are not responsible and nonfunctional requirements are also necessary for building secure web application.

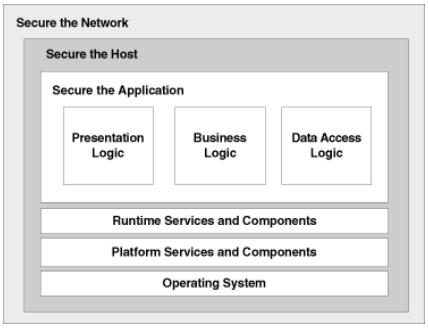

Fig.1 Secure web based application

In software engineering, a functional requirement defines a function of a software system or its component. A function is described as a set of inputs, the behavior, and outputs. Functional requirements may be calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish [3]. In another word, Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform [4]. So simply, functional requirements of a system refers to the functions of the system such as business functions, interface functions etc. [5]. Non-functional requirements are often called qualities of a system. Other terms for non-functional requirements are "constraints", "quality attributes", "quality goals", "quality of service requirements" and "non-behavioral requirements" etc. [6]. In another word, nonfunctional requirements have also been called the 'ilities' because they are most simply expressed like this: usability, reliability, interoperability, scalability, security [7]. There are several nonfunctional requirements. These are auditability, extensibility, maintainability, performance, portability, reliability, security, testability, usability and etc.

Using use case and questionnaires table, our model identify the security requirements of a system during requirement analysis phase. Where use case consists of functional requirements with actor base and questionnaires table consists of security requirements which are related to nonfunctional requirements.

J. Bangladesh Electron. 12 (1-2); 01-06, 2012

Strong Message Authentication and Confidentiality Checking Approach through Authentication Code Tied to Ciphertext

Sydul Islam Khan[1], Md. Alamgir Kabir[2], Anisur Rahman[1]
Md. Ismail Jabiullah[3] and M. Lutfar Rahman[4]

[1] Department of Computer Science and Engineering, Daffodil International University, Bangladesh
[2]Department of Software Engineering, Daffodil International University, Bangladesh
[3]Department of Computer Science and Engineering, Hamdard University Bangladesh, and
[4]Daffodil International University, Bangladesh.
[1]ksonju_cs@yahoo.com, [3]mijjabi@yahoo.com

Abstract

Message Authentication and confidentiality checking of the message are very much demanding issues in various aspects for current secured electronic transactions. A strong message authentication and confidentiality checking technique has been designed, developed and implemented using Java programming language. To do this, message is encrypted with a secret key K_1 that produces message authentication code (MAC), concatenate it with the message and again encrypted them with another secret key K_2 and again encrypted the output with key K_1 that builds the ciphertext that is to be sent to the destination. In the receiving end, first perform decryption with the secret key K_1 and then again decrypts the output with the secret key K_2 that produces the message and the MAC of the message, and then decrypts the message only to produce message authentication code MAC'; and compare the new MAC' with received message authentication code MAC that ensures the authentication of the message. Here, key values ensure the strong authentication and also confidentiality of the communicating message. It can be applied where higher-level security services of the communicating messages are needed.

Keywords: Message Authentication, Ciphertext, Secret Key, Confidentiality, Integrity and Message Authentication Code.

1. INTRODUCTION

Message authentication is a procedure that allows communicating parties to verify that received message is authentic and a message is said to be authentic when it is genuine and comes from its alleged source. An electronic transaction is best thought of as a type of electronic message that change the relationship between the sender and receiver in some important way. Electronic transactions offer speed of execution regardless of distance. They also offer accuracy and precision [1]. The key benefit of the system is a considerable potential for saving time and cost. Secure Electronic Transactions (SET) relies on the science of cryptography – the art of encoding and decoding messages. One of the reasons that encryption mechanism does not provide a good solution for message authentication is that it is difficult for the receiver to identify the legitimate plaintext. To address this problem, we can apply a process to generate a message authentication code (MAC) to the message so that only legitimate plaintext can pass the MAC detection. Such MACs are used in the network communication to provide data integrity verification against bit errors introduced by communication channel noise. But it cannot provide data integrity protection against malicious attackers. The reason is that the attackers can manipulate the message in a way which cannot be detected by MAC. Although encrypting the message and its MAC as a whole seems to be a valid approach, yet existing work shows that it still suffers from some attacks. Also it cannot solve the efficiency issue of the encryption mechanism. In light of MAC, we can design a code that uses a secret key. Without the key, modifying the message in a way that it matches the code is impossible. This idea leads to the design of MAC. Essentially, the message authentication code (MAC) is a small fixed-size block

Green University Review
ISSN 2218-5283

Life Cycle Implementation of an Android Application for Self-Communication with Increasing Efficiency, Storage Space and High Performance

Md. Alamgir Kabir[1*], Sydul Islam Khan[2] and Md. Ismail Jabiullah[3]

Keywords:
Smartphone, Linux Kernel, SDLC, Life Cycle and Android.

Abstract: Android is a Linux-based platform for mobile devices such as smartphones and tablet computers. It is developed by the Open Handset Alliance led by Google. Android delivers a complete set of software for mobile devices: an operating system, middleware and key mobile applications. In this paper, some of the phases of the system development life cycle have been implemented on android application and analyze the result of testing for efficiency, storage space and performance of the application that establishes the self-communication in mobile android applications.

1. INTRODUCTION

Android is an operating system that includes middleware and key applications. Android Inc. was founded in Palo Alto California, U.S. by Andy Rubin, Rich Miner, Nick Sears and Chris White in 2003[1-2]. Later Android Inc. was acquired by Google in 2005. After the original release there have been a number of updates to the original version of Android. There has been big barrier of broad scope of embedded devices software especially if we talk about the operating systems of embedded devices. Still abundantly used embedded devices like mobile phones are still living on proprietary operating systems, to work on those systems developers have to pay heavy prices to purchase development environment and build-linker-debugging tools. This leads to slow development in overall mobile development field, since many homebrew developers are unable to apply their research and development knowledge.

This barrier to application development began to crumble in November of 2007 when Google, under the Open Handset Alliance, released Android [3]. The Open Handset Alliance is a group of hardware and software developers, including Google, NTT DoCoMo, Sprint Nextel, and HTC, whose goal is to create a more open cell phone environment. The first product to be released under the alliance is the mobile device operating system, Android. Android is what's known as open source and, to a large degree, that means that its inner workings and machinations are free for the public to access, view and even tinker with [4]. Android will ship with a set of core applications including an email client, SMS program, calendar, maps, browser, contacts, and others. All applications are written using the Java programming language. Android was built to be truly open. For example, an application can call upon any of the phone's core functions such as making calls, sending text messages, or using the camera, allowing developers to create a richer and more cohesive experiences for users. Android is built on the open Linux Kernel [5]. Furthermore, it utilizes a custom virtual machine

[1] Md. Alamgir Kabir is with the Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh, E-mail: sagaryho@yahoo.com
[2] Sydul Islam Khan is with the Department of Computer Science and Engineering, Daffodil International University, Dhanmondi, Dhaka, Bangladesh.
[3] Md. Ismail Jabiullah is with the Department of Computer Science and Engineering, Hamdard University Bangladesh, Megnaghat, Narayangonj, Bangladesh, E-mail: mijjabi@yahoo.com
Manuscript Dates: Received: 01 December 2012; Revised: 24 December 2012; Accepted: 26 December 2012