# Intrusion Detection System for Structured Query Language Injection Attack in E-Commerce Database

**Obasi Emmanuela Chinonye Mary [*], Nlerum Promise Anebo [**]**

[*] Department of Computer Science and Informatics, Federal University Otuoke, Nigeria
[**] Department of Computer Science and Informatics, Federal University Otuoke, Nigeria

DOI: 10.29322/IJSRP.10.08.2020.p10455
http://dx.doi.org/10.29322/IJSRP.10.08.2020.p10455

***Abstract-*** The weakness of the web due to the recent trend of sophistication in cybercrime has awaken the interest of researches in securing web applications. Hence web-based information assets are not secured with increased tendency of hackers to break in. The enhancement in the features of database servers has made most of the web applications use Relational Database Management Systems (RDBMS). Attackers use SQL injection to gain unauthorized access to databases and manipulate all the valuable information stored therein. That has created interfaces that are not free from attack due to the susceptibility of risk attack in the web application called Structured Query Language (SQL) Injection. The risk of such attacks increases if the web application issues error messages each time the attacker makes an attempt. These messages guide the attacker in reconstructing SQL statement. Again, if the web application is an open source, the attacker can find potential vulnerable statements before launching the attack. The SQL injection passes SQL statements to the database directly to retrieve and/or modify valuable data. This paper focuses on the introduction of an SQL injection attack filter layer (SIAFL) to verify user inputs and filter out the known attacks. The system was modeled using Object Oriented Methodology (OOM) and developed in Visual Studio 2008 with SQL Server 2008.Windows 7 was used as the operating system

***Index Terms***- Web-based Information, Cybercrime, Hackers, Intrusion, Database, E-commerce, SQL

## I. INTRODUCTION

The invention of information technology has led to most businesses being done in the electronic platform. Applications like e-commerce and social networking create avenue for communication and rendering of online services. The ease of running most businesses online creates some loop holes that hackers exploit. There are many strategies and tactics used by hackers to steal company's valuable information. Hacking techniques that are easily used are malware, phishing, SQL Injection Attack, Cross-Site Scripting (XSS), Man –in –the Middle Attack and credential Reuse. Among all the attacks, Structured Query Language (SQL) injection attack is increasingly becoming a danger to e-businesses that operate on the web. SQL injection attack is an attack in which malicious code is inserted into application database with an intention of breaking the security authorization of that system. This method works on the principle that any constructs of SQL statements sent to the database server will be executed by the server. In 1987 Dorathy E. Denning proposed intrusion detection as an approach to counter the computer and networking attacks and misuses [1].

Generally an intruder is defined as a system, program or person who tries to and may become successful to break into an information system or perform an action not legally allowed [2]. Intrusion is referred as any set of actions that attempt to compromise the integrity, confidentiality or availability of a computer resource [3]. The act of detecting actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource can be referred to as Intrusion Detection [3]. Intrusion Detection System (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports [4].

SQL is the language for manipulating a relational database. Create, retrieve, update and delete can be done on a database using SQL. Servers that holds critical information for websites use SQL to manage the information in their databases. SQL injection attack is lunched on this kind of severs. Unfortunately, the server may divulge important information it shouldn't. This creates a big problem if private information of employers or customers such as usernames, passwords, credit cards etc are stored on such server.

When an intruder is well versed in the knowledge of SQL, he can maliciously send inputs which are not properly checked or validated by a system and that results in vulnerability that can easily be exploited. Intruding into the database via SQL injection attack has caused great damages to e-commerce. The integrity and confidentiality of data stored in the database has been compromised. In an online business, an intruder can gain access unauthorized through SQL injection attack and make changes to the prices of the commodities and make purchases. He can also make use of administrative privileges and alter important information stored in the database. This causes great loses to businesses that thrive online. These problems necessitated the need for the design and implementation of an Intrusion Detection System which is aimed at detecting and preventing SQL Injection attack form of intrusion. A Structured Query Language injection filter layer (SIAFL) is introduced to detect and filter known attacks for an online supermarket portal that sells its products online.

## II. RELATED WORKS

In order to detect and prevent SQL injection attack, many researchers had developed a variety of methods over time, since the first public discussions of SQL injection started around 1998 [5].

[6] Looked at A Closer Look at Intrusion Detection System for Web Application. The authors discussed a number of unique characteristics of the web applications and its traffic which pose challenges to designing a web IDS and explained their effects concerning the design of IDS. Their paper would highly facilitate for developers to craft an efficient architecture of the web IDS.

[7] Proposed an Online Database Intrusion Detection System Based on Query Signatures. The system they put forth was shown to protect the web application from SQL injection (SQLI). The system they proposed uses a new technique of signature- based detection. It depends on secure hash algorithm (SHA-I), which is used to check the signature for submitted queries and to decide the validity or invalidity of submitted queries. The system proposed can differentiate and prevent attempts by hackers through detection of the attacker, blocking his/her request and ensuring he/she is prevented from accessing the web application again. Sqlmapproject attacking tool was used to test the proposed system. The web application was attacked with Sqlmapproject (built using PHP and MySQL server) before and after protection. The results showed that the proposed system works correctly and it can protect the web application system with good performance and high efficiency.

[8] Presented an efficient method that the detection of SQL injection is done by tampering with the input features of query strings, analysis of query relating to the sustainability for both static and dynamic manipulation of users queries.

[9]Surveyed paper on intrusion detection techniques. There focus was on detection method to increase the detection rate and help the users to develop information systems that are secured. The different methods for intrusion detection discussed were Pattern Matching, State Full Pattern Matching, Protocol Decode-based Analysis, and Fuzzy Clustering for IDS. They also presented a four step approach for the generalized working of IDS to include Data collection, Feature selection, Analysis and Action.

[10]Created a schema, (SQLshield) that changes the data inputted by the user before the SQL query is sent to the database server .It deploys a randomization technique. This techniques makes it impossible for the execution outcome of SQL query to deviate from its programmer intended execution.

[11] Proposed a misuse detection system called (DEMIDS) which was meant for relational database systems.

[12] Worked on A Review of Intrusion Detection Systems. They reviewed some of the intrusion detection systems and softwares, highlighting their main classifications and their performance evaluations and measures. They concluded that selecting and implementing a Network Intrusion Detection System is a challenging task. To ensure a successful implantation, an organization should determine its requirements and then locate a system that meets them.

## III. METHODOLOGY

### 3.1. Research Design.

The adopted methodology for the proposed system design is the Water-fall Model. Waterfall Model is a sequential model that divides software development into different phases. Each phase is designed for performing specific activity during SDLC (Software Development Lifecycle Methodology) phase.

### 3.2 Analysis of the Existing System

SQL injection attack is the type of attack that takes place in web application that executes SQL statements. These statements are launched by a database server that works with web application. Hackers can use it to gain access to sensitive information such as personal business secrets, personal discoveries, account details and so on. They can use it to skip authentication and authorization of a web page and retrieve all information stored in the database. SQL injection attack can be used to add, modify and delete records in the database.

In online Kiddies Supermarket, the portal administrator uses his privilege to log into the admin module and make changes on the product name and prices. The buyers buy at the right prices using the appropriate channel. The e-commerce database is vulnerable to SQL injection attack because there is no SQL Injection Attack Filter Layer.

The attack buyer, through an SQL injection attack issues query to the database, changes the usernames and passwords and alters the price of a commodity from N150,000 to N150 so as to buy at a much reduced rate as shown in the figure 3.1 below. The attack buyer can change this information by carefully exploiting the vulnerability of a SQL injection. He can inject SQL command as an input through web pages and change the contents of the database and prices of commodities. This will reduce the confidentiality of the database since the sensitive data in the database that can be altered with ease.

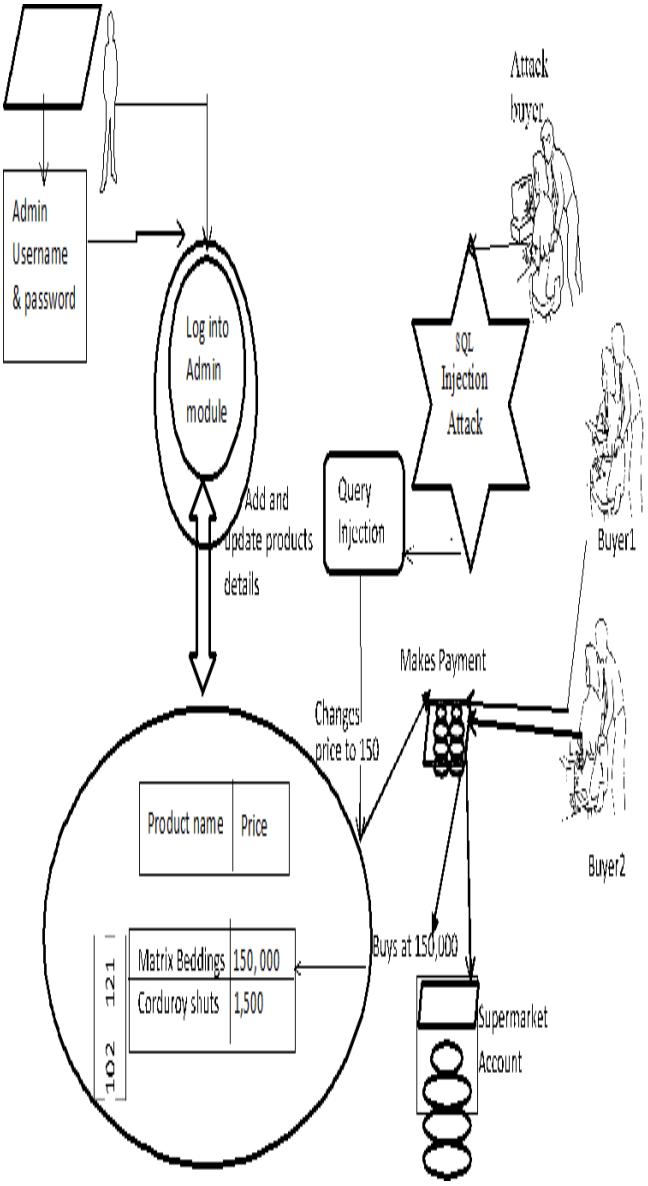



Figure 3.1: Existing System Architecture.

### 3.2.1 Disadvantages of the Existing System

The disadvantages of the Existing System are:

- SQL injection attack usually affects sites that uses an SQL database such as MYSQL, Oracle, SQL server or others.
- SQL injection attack that is launched successfully can result in loss of confidential data.
- Alteration of data in an online business through SQL injection can lead to great loss.

### 3.3 Analysis of the Proposed System

Electronic commerce, commonly known as (electronic marketing) e-commerce consists of the buying and selling of products or services over electronic systems such as the internet and other computer network [13]. SQL injection attack in E-commerce is a trick to inject SQL query/command as an input possibly via web pages in order to change the database contents and select the price of the commodities. Many web pages take parameters from webpage, and make SQL query to the database. Take for instance when a user logs in, the web page that contains user name and password makes SQL query to the database to check if a user has valid name and password. With SQL injection, it is possible for an attacker to send crafted user name and password field that will change the SQL query and grant something else.

The first part in developing an intrusion detection system for e-commerce was to develop an online shopping of Kiddies supermarket. The online supermarket was developed using ASP.Net which is an advanced software for developing web applications. A customer makes his transactions online and enters his details including the credit card information for online delivery. Making changes to the Kiddies Supermarket website or the database is being done by a web master administration or those with privileges to make changes. The administrator enters his username and password before he is granted access to the software. When an authorized customer submits his credentials, an SQL query is generated from these details and submitted to the database for verification. If valid, the user is allowed access. In order words, the web application that controls the login page will communicate with the database through a series of planned commands so as to verify the username and password combination.

.

By means of SQL injection, the hacker may put in well-constructed SQL commands in a specific manner with the purpose of diverting the login form barrier and seeing what lies at the back of it. This opportunity is achievable only if the inputs are not well scrutinized and sent alongside with the SQL query to the database. SQL injection susceptibility to attack provides the means for a hacker to pass on information in order to alter the records in a database. The technologies that easily fall prey to this attack are dynamic script languages including ASP, ASP.NET, PHP etc.

In the proposed system, there is an introduction of an SQL injection attack filter layer (SIAFL) to filter out the know attacks. The Object Oriented Methodology (OOM) was used for this system development. The rationale behind OOM is to design the logical design from a physical design based on noting and recording the features of the "real world". OOM is a new system development approach encouraging and facilitating re-use of software components. This methodology can be used to design and implement a robust system based on reuse of codes of existing component and this makes easy the sharing of its small units by other systems. The architecture of the proposed system is shown in the figure 3.2

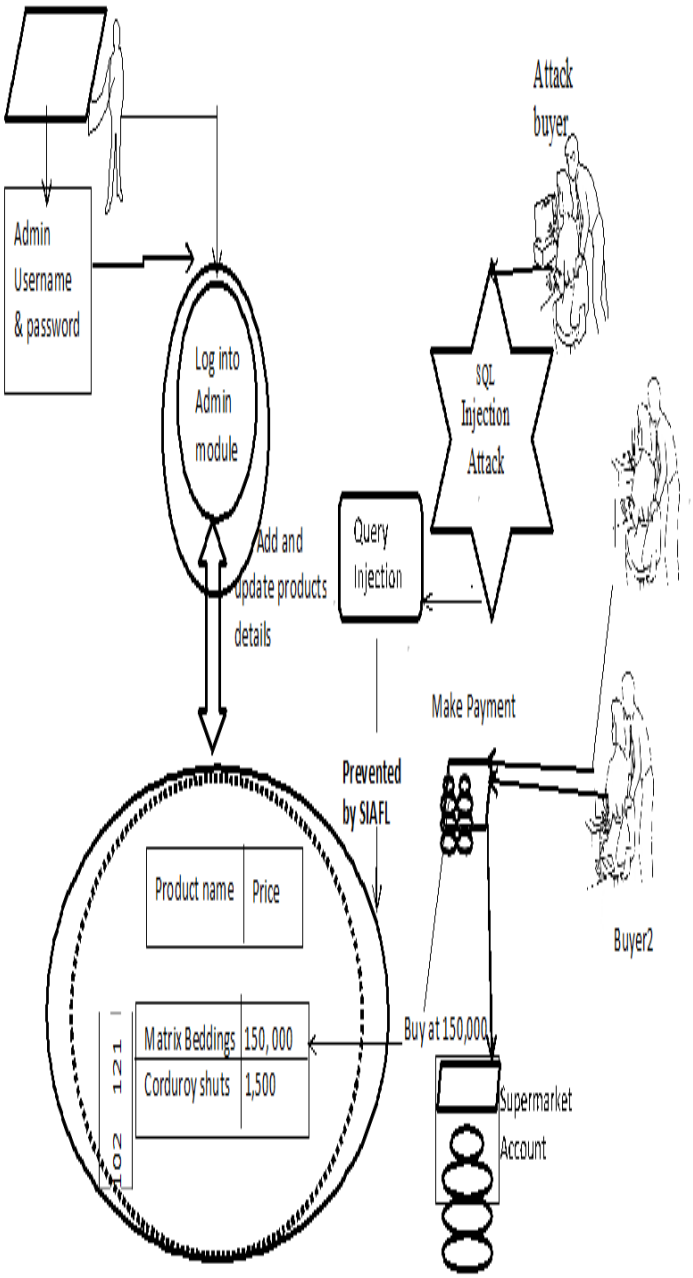



Figure 3.2: Proposed System Architecture

### 3.3.1. Advantages of the Proposed System Components

The following advantages of the Proposed System are:

i) SQL injection attack filter layer (SIAFL) caries out data sanitation and validation

ii It blocks and prevents alterations to data.

Iii Hackers are denied knowledge of database structure which usually comes from error messages.

## 3.4. Overall System Flowchart of the Proposed Intrusion Detection System

### 3.4.1. The System Flowchart of the Online Shopping Transaction.

The Flowchart of the Online Shopping Transaction is shown in figure 3.3.

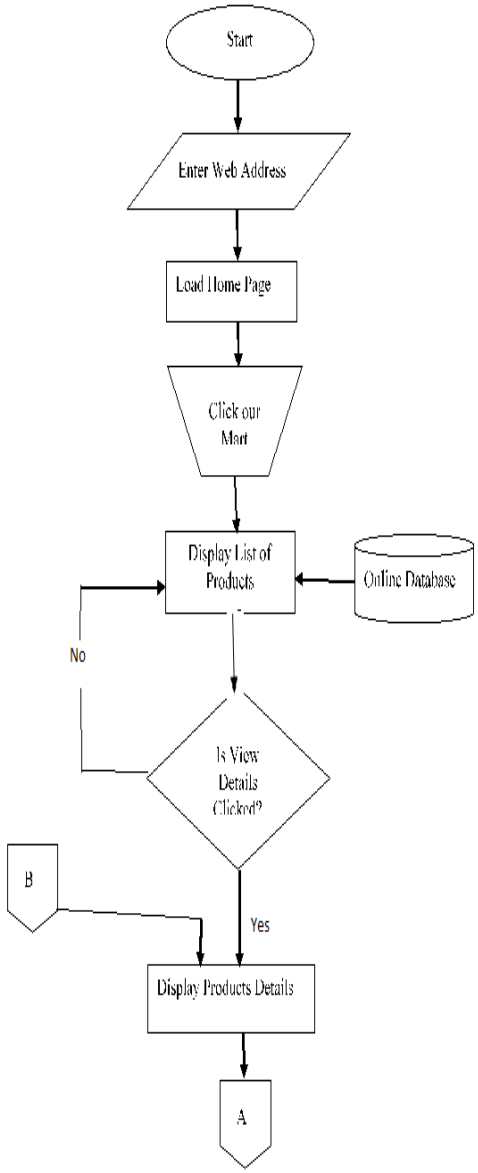
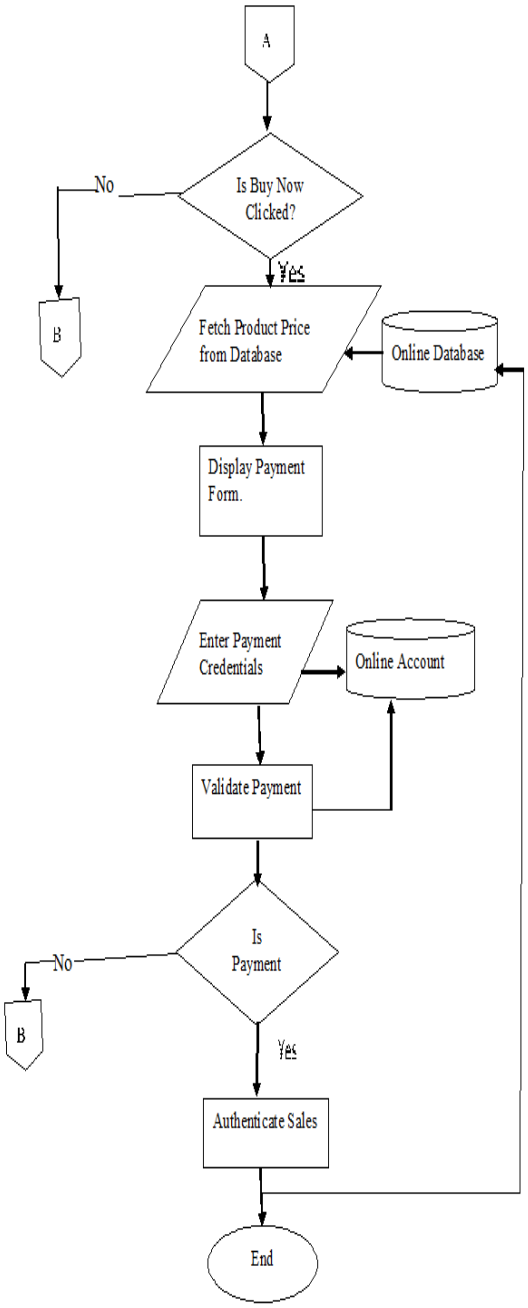
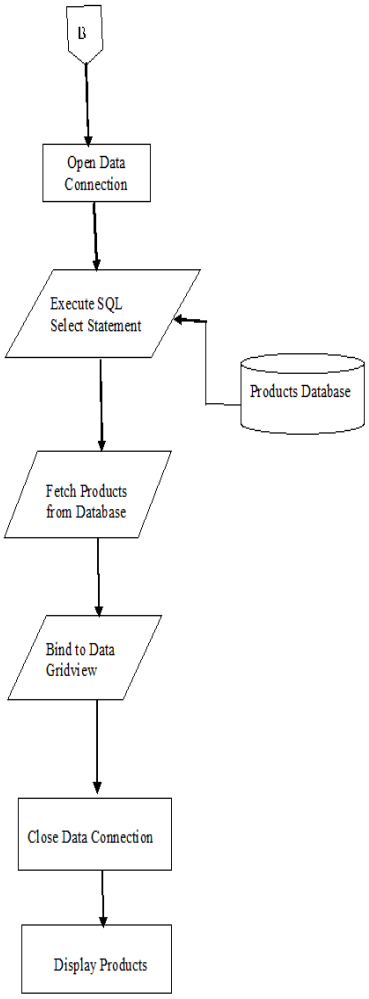



Figure 3.3. System Flowchart of the Online Shopping Transaction.




### 3.4.2. SQL Injection Attack Prevention Flowchart.

The flowchart for SQL Injection Attack Filter Layer in figure 3.4

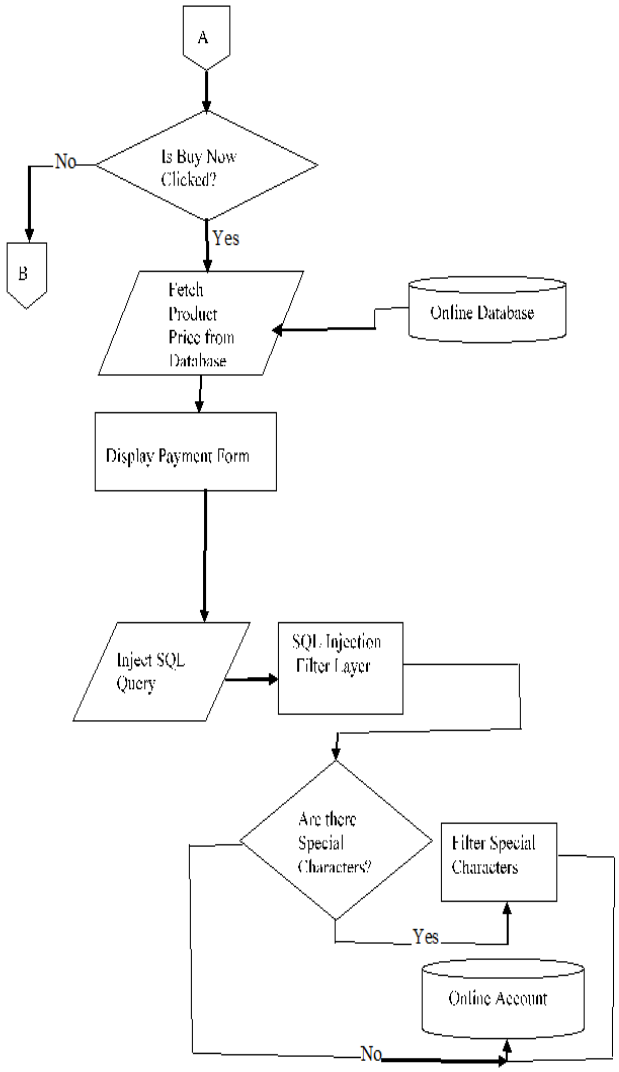



Figure 3.4. System Flowchart of SQL Injection Attack Filter Layer

## IV. IMPLEMENTATION AND SAMPLE RESULTS

Following the system architecture, database design and Object Oriented Methodology, the system coding was achieved. Microsoft SQL 2008 server was used as a Database Management System. A new database named Online Supermarket Database was created using the SQL Server Enterprise Manager Panel. The following tables and their corresponding parameters were created for the database.

- dbo.CardType
- dbo.Category
- dbo.Products
- dbo.Purchase
- dbo.PurchaseDetails
- dbo.State
- dbo.Users

To access the web pages, Internet Information System was installed on the machine for hosting the web pages. The website was built using ASP.NET. ASP.NET was used to create web pages and web technologies and is an integral part of Microsoft's .NET framework vision. Graphical Interfaces Creation were created as modules to give the various methods the expected parameters. Visual Studio was used as a tool for designing the interfaces using the control toolbox which consists of textbox, image buttons, labels etc. The system was tested and some sample outputs (screen shots) as depicted in figure (a-c) were obtained respectively.

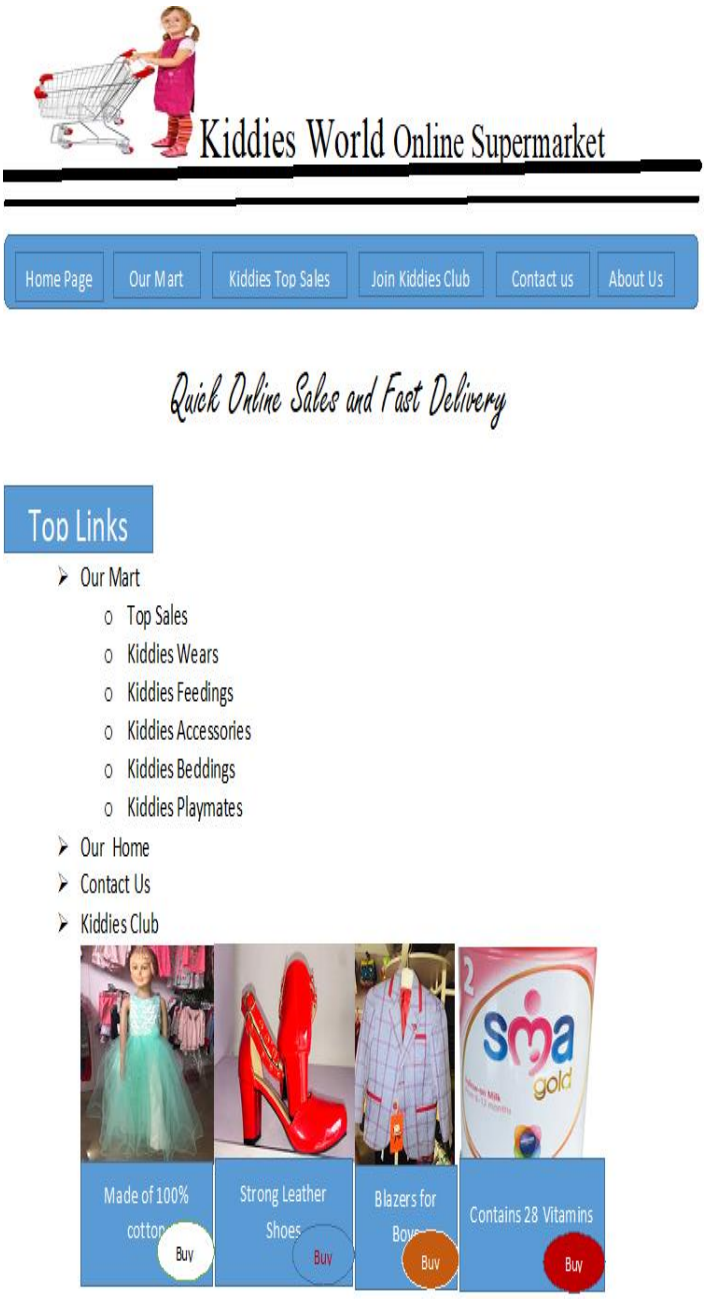



Figure 4.0 (a): Home Page for Online Kiddies Supermarket.



Figure 4.0 (b): Payment Details for Goods Bought


Figure 4.0 (c): Admin Login Page with SQL Injection Attack Filter Layer

## V. CONCLUSION

If an attacker can construct an SQL syntax correctly and launched it on a database server, he or she can succeed in carrying out SQL Injection Attack. Once an incorrect query is sent to a database server, an error message will be generated. The attacker will read the error message generated as a result of the incorrect query. This will guild him to construct again the logic of the original query and then he will understand how to perform the injection correctly. The SQL Injection Attack Filter Layer (SIAFL) has proved to be successful in detecting SQL injection attack in e-commerce. With this, there is significant level of reliability in online businesses.

## REFERENCES

[1] Botha M., R.Solms,"Utilizing neural networks for effective intrusion detection,"ISSA.2004

[2] Graham. R., "FAQ: Network intrusion detection systems" 2000

[3] Zamboni D., "Using internal sensors for computer intrusion detection," Center for Education and Research in Information Assurance and Security, Purdue University. 2001

[4] Scarfone K., P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," Computer Security Resource Center (National institute of standards and technology).2007

[5] Kerner S.M.,How was SQL Injection Discovered? In eSecurity.2013

[6] Nancy A. and Syed Z.H, A Closer Look at Intrusion Detection System for Web Applications. Hindawi Security and communication Networks. 2018

[7] Alaa K.J and A.O. Awezan, Online Database Intrusion Detection System Based on Query Signatures. Journal of University of Human Development. 3(1) 282-287.2017

[8] Latha R and E. Ramaraj , SQL Injection Detection Based on Replacing the SQL Query Parameter Values, International Journal of Advanced Trends in Computer Science and Engineering.2015

[9] Rachna Kulhare, Divakar Singh, Survey paper on Intrusion Detection Techniques, International Journal of Computers and Technology.6 (2).329-335.2013

[10] Mehta P., J.Sharda and M. L. Das, SQLshield: Preventing SQL Injection Attacks by modyfying User Input Data in International Conference on Information Systems Security.2015

[11] Chung C.Y, M.Gertz, and K.Levitt. Demids: A Misuse Detection System for Database
Systems in Integrity and Internal Control in Information Systems. Springer. 159-178. 2000

[12] Neyole M.J. and Muchelule Y.W.), A Review of Intrusion Detection Systems. International Jlurnal of Computer Science and Information Technology Reseach.5(4), 1-5. 2017

[13] Chauudhury Ability, Jean – Perre Kuibboer, "e-business and e-commerce infrastructure," McGraw Hill. 2000

## AUTHORS

**First Author** – Obasi Emmanuela Chinonye Mary, B.Tech Computer Science, Second Class Upper Division, MSc. Computer Science, PhD Computer Science (in view), Lectures at Federal University Otuoke, Bayelsa State, Nigeria. anchinos@yahoo.co.uk

**Second Author** – Nlerum Promise Anebo, B.Sc Computer Science, Second Class Upper Division, MSc. Computer Science, PhD Computer Science, Lectures at Federal University Otuoke ,Bayelsa State, Nigeria. nlerumpa@fuotuoke.edu.ng

**Correspondence Author** – Obasi Emmanuela Chinonye Mary, anchinos@yahoo.co.uk, obasichinonye20@gmail.com
, 07036673665