

**PROJECT REPORT**  
**SQL INJECTION DETECTION AND PREVENTION**

*Submitted by partial fulfillment of requirement for the award*

*of the degree of*

**BSC Cyber Forensic**

Done by

**AKSA ANNA SHAJAN – 170021022927**

**ARSHA MARY ISSAC – 170021022936**

**SRUTHI R -170021022952**

Under the guidance of

**Ms. Alphonsa Sini P.J**

Lecturer

**STAS , EDAPPALLY**



**2017-2020**

**CENTRE FOR PROFESSIONAL AND ADVANCED STUDIES**  
**SCHOOL OF TECHNOLOGY AND APPLIED SCIENCES**

**CENTRE FOR PROFESSIONAL AND ADVANCED STUDIES  
SCHOOL OF TECHNOLOGY AND APPLIED SCIENCES**



**CERTIFICATE**

This is to certify that the project entitled “**SQL INJECTION DETECTION AND PREVENTION**” is a bonafide work done by **ARSHA MARY ISSAC** submitted in the partial fulfillment of the requirement of the degree of Bsc. Cyber Forensic of School Of Technology And Applied Sciences Edappally

Course Co-ordinator

Lecture in charge

External Examiner

Internal Examiner

### **ACKNOWLEDGEMENT**

A project work done is a product of experience that a person needs to build up in respective profession. That is not of his merit but a group of heart is behind the success. If words are considered as the symbol of approval and tokens of acknowledge them the words play the heralding role of expression my gratitude.

First of all, I thank the **ALMIGHTY** for showering his grace and blessing upon me to carry throughout, from the very beginning when I took up the work till very submission of work

We would like to express my sense of gratitude towards **Dr BINDHU K,Principal School Of Technology And Applied Sciences, Edappally** for providing the necessary resources for the completion of this project.

We extend our sincere and heartfelt thanks to **Ms. NISSA S.S , Course Coordinator** of Cyber Forensics for providing us an opportunity to present the project at its best.

We also express our deep gratitude to the faculty member **Ms. ALPHONSA SINI** for her valuable guidance, timely suggestions and help in the completion of this project

We extend our sincere thanks to all the teaching and non-teaching staff for providing the necessary facilities and help. Last, but not the least. We would like to thank all our friends and well-wishers for their support and prayers.

**ARSHA MARY ISSAC**

## **DECLARATION**

We, hereby declare that the mini project report “**SQL INJECTION DETECTION AND PREVENTION**” is submitted in partial fulfillment of the requirements for the fifth semester of Bachelor of Science and it is a report of the original work done by us in the department of cyber forensics of MG university School of Technology and Applied Sciences, Edappally.

Place: Edappally

Date:

**ARSHA MARY ISSAC**

## **ABSTRACT**

SQL Injection Attack (SQLIA) is a type of code injection technique that threatens confidentiality, integrity, and availability of web databases. The attacker mostly exploits incorrectly filtered user inputs such as text fields in web applications and tries to insert malicious SQL statements into a legitimate query via the vulnerable user input. By doing so, the attacker can access, insert, modify, or delete critical information in a database without proper authorization. In this survey, we describe and categorize types of SQLIA, and analyze existing detection and prevention techniques against such attacks

## CONTENTS

<b>1.INTRODUCTION</b>	8
<b>2.SYSTEM STUDY</b>	9
2.1 EXISTING SYSTEM	9
2.2 PROPOSED SYSTEM	9
2.2.1 MODULAR DESCRIPTION	10
2.2.2 DATA FLOW DIAGRAM	11
<b>3. SYSTEM SPECIFICATION</b>	13
3.1 SOFTWARE SPECIFICATION	13
3.2 HARDWARE SPECIFICATION	13
<b>4. SYSTEM ANALYSIS</b>	14
4.1 FEASIBILITY STUDY	14
4.1.1 TECHNICAL FEASIBILITY	14
4.1.2 OPERATIONAL FEASIBILITY	15
4.1.3 ECONOMIC FEASIBILITY	15
4.1.4 BEHAVIOURAL FEASIBILITY	16
<b>5. SYSTEM DESIGN</b>	17
5.1 INPUT DESIGN	17
5.2 OUTPUT DESIGN	17
5.3 TABLE DESIGN	18
5.4 SYSTEM ARCHITECTURE	20
<b>6. TECHNOLOGY PROFILE</b>	21
6.1 C#	21
6.2 SQL	21
6.3 DESIGN	22
6.4 VISUAL STUDIO	23
<b>7.SYSTEM TESTING</b>	24
7.1 UNIT TESTING	25
7.2 INTEGRATION TESTING	26
7.3 VALIDATION TESTING	26
7.4 USER ACCEPANTANCE TESTING	27
<b>8. CONCLUSION</b>	28

<b>9. FUTURE ENHANCEMENT</b>	28
<b>10. RFFERENCE</b>	29
<b>11. APPENDIX</b>	30
11.1 SCREENSHOTS	31

## **1. INTRODUCTION**

SQL injection attack is widely used by attackers to gain unauthorized access to systems. This software system is developed to prevent unauthorized access to system using SQL injection attacks. This is done by adding unique value and a signature based authentication technique to verify authenticity. SQL injection is a major security issue these days that allows an attacker to gain access of a web system or application exploiting certain vulnerabilities. This method exploits various web application parameters such as transmitting the traveling form data parameters with an efficient integration of amino acid codes aligned in it. In other words, this software project puts forth a method to analyze and detect the malicious code to find out and prevent the attack. It uses an alternative algorithm for signature based scanning method; this method is based on a different divide and conquers strategy that detects attacks based on various time/space parameters. This innovative system has proved successful in preventing various SQL injection attacks based on its efficient attack detection strategies.



## **2.SYSTEM STUDY**

### **2.1 EXISTING SYSTEM**

SQL injection is a type of security exploit in which the attacker adds Structured Query Language (SQL) code to a Web form input box to gain access to resources or make changes to data. An SQL query is a request for some action to be performed on a database. Typically, on a Web form for user authentication, when a user enters their name and password into the text boxes provided for them, those values are inserted into a SELECT query. If the values entered are found as expected, the user is allowed access; if they aren't found, access is denied.

However, most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.

### **DISADVANTAGES OF EXISTING SYSTEM**

- An attacker might insert a SQL query as input to perform an unauthorized operation
- Using SQL injection attacks, an attacker can retrieve or modify confidential and sensitive information from the database.
- SQL-injection attacks make weak validation of input used to build database queries.

### **2.2 PROPOSED SYSTEM**

The project is created as a web application which provides more security and integrity. Admin can login and get the users list details which includes ip address along with time of login. SQL injection attacks are prevented by making username in a specific format(eg: [abc@gmail.com](mailto:abc@gmail.com)). Any query entered which is not in that particular format will be considered invalid. Brute force attack and DDos attacks are prevented by providing a fixed number of attempts for a particular login, which is set by the admin. Trying to login more than the limit will result in access denial

### **ADVANTAGES OF PROPOSED SYSTEM**

- Prevention of SQL Injection.
- Detects malicious code when anyone tries to input using SQL Injection.
- Prevention of brute force attack and DDos

### **2.2.1 MODULE DESCRIPTION**

Project is divided into following modules

- Admin login
- User login/Registration
- Attack

#### **ADMIN LOGIN**

This module includes admin login and certain other features. Admin can see the visitors list. It includes users details along with IP address and login time.

**Prevention:** sql injection attacks are prevented by providing particular format for username. Brute force attack and DDos attacks are also prevented by blocking login after a particular number of trial.

#### **USER LOGIN/REGISTRATION**

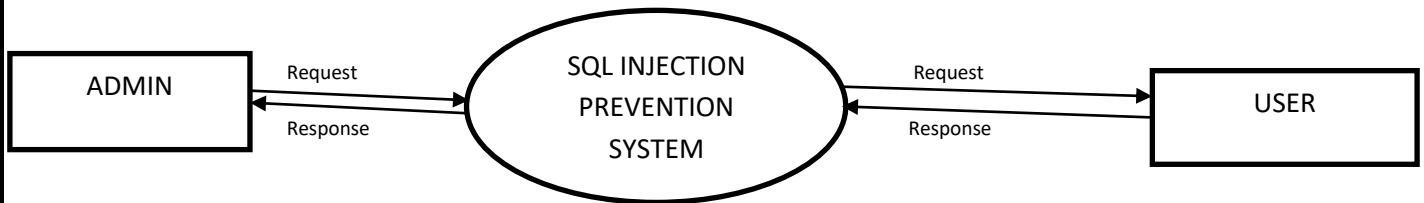
In this module a new user can register by submitting the registration form. User can further login whenever required.

#### **ATTACK**

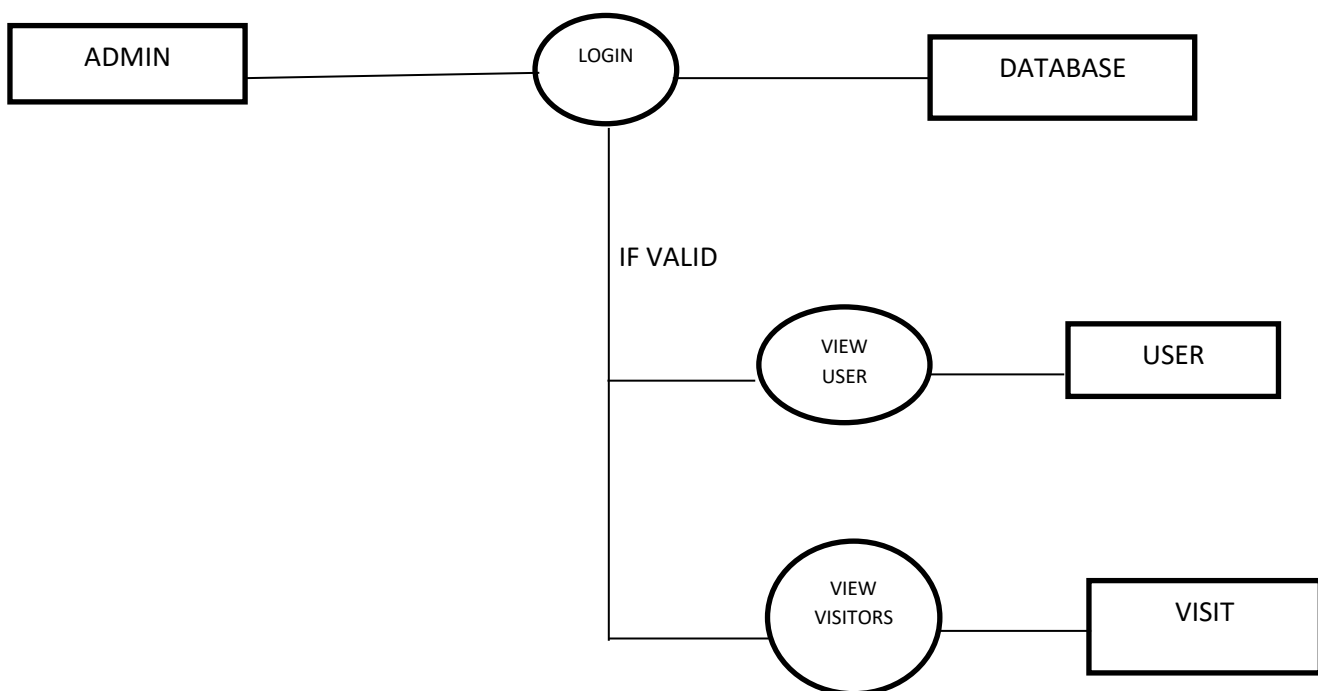
sql injection attacks are done using Select , insert and delete queries.

### 2.2.2 DATA FLOW DIAGRAM

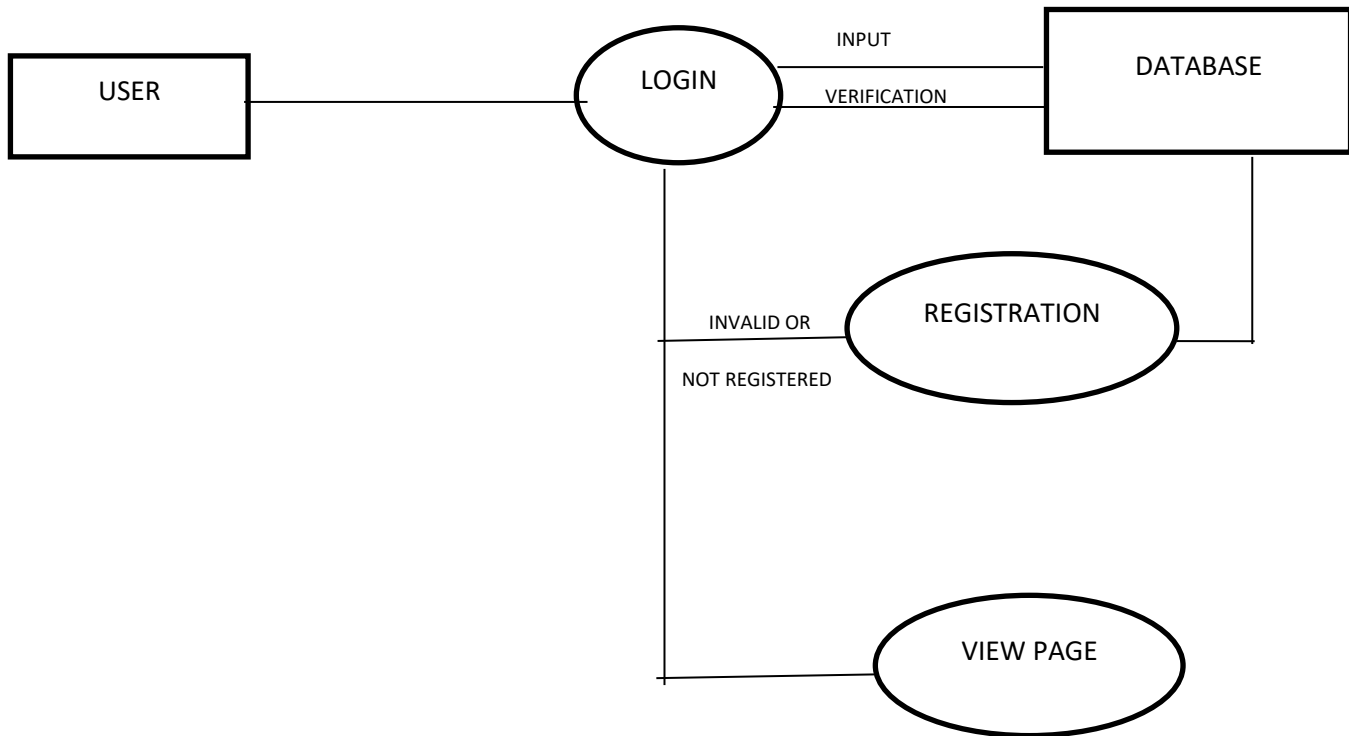
#### LEVEL 0 DFD



#### LEVEL 1 DFD



## LEVEL 1 DFD



### **3. SYSTEM SPECIFICATION**

#### **Software Requirements:**

- Windows 7 or higher
- Microsoft SQL Server 2008
- Visual Studio 2010

#### **Hardware Components:**

- Processor –Core i3
- Hard Disk – 300 GB
- Memory – 2GB RAM
- Monitor

## **4. SYSTEM ANALYSIS**

### **4.1 FEASIBILITY STUDY**

The main goal of feasibility study is to assess the economic viability of the proposed “Does the idea make economic sense?”. The study should provide a thorough analysis of the system. The outcome of the feasibility study will indicate whether or not to proceed with the proposed venture. If the results of the feasibility study are positive, then the co- operative can proceed to develop a business plan. Feasibility analysis is the procedure for identifying the candidate system, evaluating and electing the most feasible system. Feasibility analysis is initiated when users within an organization face the need for change or improvement in the current system, which could be either manual or automated. A feasibility study could be used to test a new working system, which could be because business. The feasibility study needs to answer the question:

- The current system may no longer suit its purpose,
- Technological advancement may have rendered the current system obsolete.

When a new project proposed, it normally goes through feasibility assessment.

Feasibility study is carried out to determine whether the proposed system is possible to develop with available resources and what should be the cost consideration.

Facts considered in the feasibility analysis were:

- Technical feasibility
- Operational feasibility
- Economic feasibility
- Behavioral feasibility

#### **4.1.1 Technical Feasibility**

Technical feasibility is frequently the most difficult area to assess at the system development process stage. It centers on the existing computer system (hardware, software etc ) and to what extent it can support the proposed addition. This involves financial consideration to accommodate technical enhancement. It is essential that the process of analysis and definition be conducted in parallel with an assessment of technical feasibility In this way concrete

specification may be judged, as they are determined. This system is technically feasible.

#### 4.1.2 Operational Feasibility

Proposed projects are beneficial only if they can be turned into information systems that will meet the organization's operating requirements. Simply, there is no difficulty in implementing the system if the user has knowledge. The purpose of the operational feasibility study is to determine whether the new system will be used if it is to be developed and implemented, and whether there will be resistance from users that will undermine the possible application benefits.

There was no difficulty in implementing the system and the proposed system is so effective, user friendly and functionally reliable that the users in the company will find that the system reduce their hardships. If the users of the system are fully aware of the internal working of the system then users will not be facing any problem in running the system.

#### 4.1.3 Economic Feasibility

Economic analysis is the most important and frequently used method for evaluating the effectiveness of the proposed system, it is very essential because the main goal of the proposed system is to have economically better result along with the increased efficiency. Economic analysis is the most commonly used method for evaluating effectiveness of the system. Cost-benefit analysis is the most important assessment of the economic justification of the project.

Cost-benefit analysis delineates the cost for project development and weighs them against tangible and intangible benefits of the system, the relative size of the project, and the expected return on the investment desired as a part of company's strategic plan. Benefits of a system are always determined relative to the existing mode of operation.

This system is economically feasible since it does not require any initial setup cost. It does not need additional staffing requirements. Economic feasibility deals about the economic impact faced by the organization to implement a new system. Not only cost of hardware, software etc is considered but also the form of reduced cost. The project, installed, certainly be beneficial since there will be a reduction.

#### 4.1.4 Behavioral Feasibility

The system does not require much maintenance once it is implemented. As the system is fully GUI based so it would be easy for the user to get friendly with the system. The user need not be a computer professional. The system is equipped with various design tools so that the user can make use of these as when we required , thus needing less help from outside for maintenance the system.

#### Feasibility Study Process

Feasibility study comprises the following steps

1. **Information Assessment:** Identifies information about whether the system helps in achieving the objective of the organization. It also verifies that the system can be implemented using new technology and within the budget, and whether the system can be integrated with the existing system.
2. **Information Collection:** Specifies the sources from where information about software can be obtained. Generally, this source include users, and the software development team
3. **Report Writing:** Users a feasibility report, which is the conclusion of the feasibility by the software development team. In includes the recommendation whether the software development should continue or not



## **5. SYSTEM DESIGN**

### **5.1 INPUT DESIGN**

The input design is the link between the information system and the user. It comprises developing specification and procedures for data preparation and those steps that are necessary to put transaction data into a usable form for processing data entry. Instructing the computer to read data from a written or a printed document can achieve the activity of putting data into the computer for processing or it can occur by having people key data directly into the system. The design of inputs focuses on controlling the amount of inputs required, controlling errors, avoiding extra steps and keeping the process simple. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A larger number of problems with a system can usually be traced back to fault input design and method. Needless to say, therefore that the input data is the life block of a system and has to be analyzed and designed with the most consideration. It is the process of converting the user-oriented inputs in to the computer-based format. The goal of designing input data is to make the automation as easy and free from errors as possible. For providing a good input design for the application easy data input and selection features are adopted. The input design requirements such as user friendliness, consistent format and interactive dialogue for giving the right message and help for the user at right time are also considered for the development of the project. In this project all textboxes are validated. If any field is not filled then it will display an error message that the field is blank. List boxes are used to reduce the user inputs.

### **5.2 OUTPUT DESIGN**

In output design the emphasis is given on producing a hard copy of the information required as the output on the screen in some predefined manner. Computer output is the most important process that involves designing necessary outputs that should be given to various users according to their requirements. Efficient intelligible output design should improve system relationship with the user and help in decision making.

Only software needed to operate this site. This site is optimized to work with various browsers. Special extension for individual browsers is avoided for the unique performance. A unique colorings screen gives the user and integral feeling for the entire site. Proper help and user-friendly message are given to the user to avoid confusion.

Forms are designed with GUI designed tools like textboxes, List boxes, Radio Button, Checkbox...etc. which are very user Friendly and self-explanatory. Proper validations are given to the textboxes with user understandable error messages which helps the user to correct it and submit again.

The data in the system is stored and retrieved from the database. Designing the database is a part of the system design. Data elements and data structures to be stored have been identified at analysis stage. They are structured and put together to design the data storage and retrieval system. The general theme behind the database is to handle the information as an integrated whole. When designing the database, we have to make decisions regarding how best to make some systems in the real world and model it as database.

The overall objective in the development of database technology has been to treat data as an organizational resource and as an integrated whole. DBMS allow data to be protected and organized separately from other resources. Database is an integrated collection of data. The most significant form of data as seen by the programmers is data as stored on the direct access storage devices. This is the difference between logical and physical design.

Database files are the key source of information in to the system. It is the process of designing database files, which are the key source of information to the system. The files should be properly designed and planned for collection, accumulation, editing and retrieving the required information. This database contains tables, where each table corresponds to one particular type of information. Each piece of information in the table is called a field or column. A table also contains records, which is a set of fields. All records in a table have the same set of fields with different information. There are primary key fields that uniquely identify a record tab

### 5.3 TABLE DESIGN

TABLE NAME: **tbl\_users**

FOREIGN KEY: **UserId**

COLUMN	DATA TYPE	DESCRIPTION
UserId	int	User id
UserName	Varchar(100)	Name of User
password	Varchar(100)	Password of User
UserType	Varchar(100)	Type of user

TABLE NAME :**tbl\_Registration**

PRIMARY KEY:UserId

COLUMN	DATA TYPE	DESCRIPTION
ID	Int	Identify column
Name	Varchar(100)	User Name
Address	Varchar(MAX)	User Address
Sex	Varchar(50)	Gender
MobNo	Varchar(100)	Mobile Number
Email	Varchar(100)	Email Id
UserId	Int	User Id

TABLE NAME:**tbl\_LoginHistory**

FOREIGN KEY: UserId

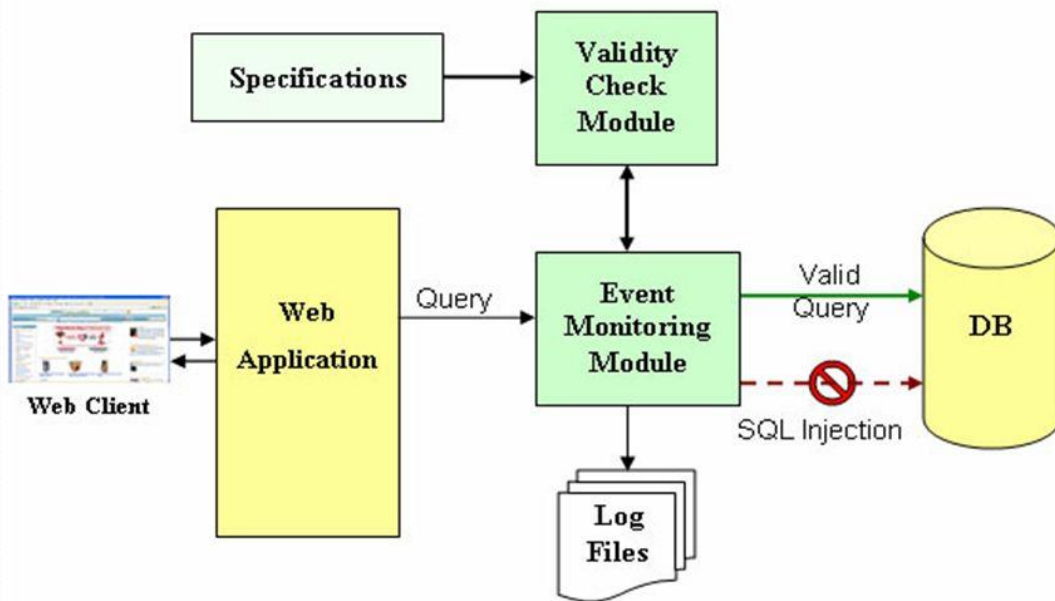
COLUMN	DATA TYPE	DESCRIPTION
Id	Int	Identify column
UserId	Int	User Id
IpAddress	Varchar(MAX)	User IP Address
Time	Varchar(100)	Time of Login
Date	Varchar(100)	Date of Login

TABLE NAME:**tbl\_Attack**

COLUMN	DATA TYPE	DESCRIPTION
Id	Int	Identify column
AttackCount	Varchar(50)	Max Attempt

## 5.4 SYSTEM ARCHITECTURE

### System Architecture



## **6. TECHNOLOGY PROFILE**

### **6.1 C#**

C-sharp is one of the most important languages used in the .Net Environment. It is a whole new language free of the background compatibility curse with a whole bunch of new, exciting and promising features. It is an object oriented programming language and has at its core, many similarities in java, c# and visual. In fact, c# combines the power and efficiency of c++, the simple and clean object oriented design of java and the language simplification of visual Basic. Like java, C-sharp also does not allow multiple inheritances or the use of pointers but provide garbage memory collection at runtime, type , memory access checking.

#### **Features of C#**

- C# is a simple, modern, object oriented language derived from C++ and java
- It aims to combine the high productivity of visual Basic and raw power of C++.
- It is a part of Microsoft Visual Studio 7.0.
- Visual Studio supports VB,VC++,C++, VB Script, J Script. All of these languages provide access to the Microsoft .NET platform.
- .NET includes a Common Execution engine and rich class library.

### **6.2 SQL**

SQL (pronounced "ess-que-el") stands for Structured Query Language. SQL is used to communicate with a database. According to ANSI (American National Standards Institute), it is the standard language for relational database management systems. SQL statements are used to perform tasks such as update data on a database, or retrieve data from a database. Some common relational database management systems that use SQL are: Oracle, Sybase, Microsoft SQL Server, Access, Ingres, etc. Although most database systems use SQL, most of them also have their own

additional proprietary extensions that are usually only used on their system. However, the standard SQL commands such as "Select", "Insert", "Update", "Delete", "Create", and "Drop" can be used to accomplish almost everything that one needs to do with a database. This tutorial will provide you with the instruction on the basics of each of these commands as well as allow you to put them to practice using the SQL Interpreter.

### 6.3 DESIGN

Client-Server database management systems, The SQL engine has no standalone processes with which the application program communicates. Instead, the SQL library is linked in and thus becomes an integral part of the application program. The library can also be called dynamically. The application program uses SQL functionality through simple function calls, which reduce latency in database access: functions called in a single process are more efficient than inter-process communication. SQL stores the entire database (definitions, tables, indices, and the data itself) as a single cross-platform file on a host machine. It implements this simple design by locking the entire database file during writing. SQL read operation can be multitasked, though writes can only be performed sequentially.

Due to the server-less design, SQL applications require fewer configurations than client-server databases. SQL is called *zero-conf* because it does not require service management (such as startup scripts) or access control based on GRANT and passwords. Access control is handled by means of File system permissions given to the database file itself. Databases in client-server systems use file system permissions which give access to the database file only to the daemon process.

Another implication of the server less design is that may need to be able to write to the database file. In server-based databases, several writers will all connect to the same daemon, which is able to handle its lock internally. SQL on the other hand has to rely on file-system locks. It has less knowledge of the other processes that are accessing the database at the same time. Therefore, SQL is not the preferred choice for write-intensive deployments. However, for simple queries with little concurrency, SQL performance profits from avoiding the overhead of passing its data to another process.

SQL uses PostgreSQL as reference platform. “What would PostgreSQL do” is used to make sense of the SQL standard. One major deviation is that, with the exception of primary keys, SQL does not enforce type checking; the type of a value is dynamic and not strictly constrained by the schema (although the schema will trigger a conversion when storing, if such a conversion is potentially reversible). SQL strives to follow Postel’s Rule.

#### **6.4 Visual Studio**

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web apps, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code.

Visual Studio includes a code editor supporting IntelliSense (the code completion component) as well as code refactoring. The integrated debugger works both as a source- level debugger and a machine-level debugger. Other built-in tools include a code profiler, forms designer for building GUI applications, web designer, class designer, and database schema designer. It accepts plug-ins that enhance the functionality at almost every level— including adding support for source control systems (like Subversion) and adding new toolsets like editors and visual designers for domain-specific languages or toolsets for other aspects of the software development lifecycle (like the Team Foundation Server client: Team Explorer).

Visual Studio supports 36 different programming languages and allows the code editor and debugger to support (to varying degrees) nearly any programming language, provided a language-specific service exists. Built-in languages include C,[6] C++ and C++/CLI (via Visual C++), VB.NET (via Visual Basic .NET), C# (via Visual C#), F# (as of Visual Studio 2010[7]) and Type Script (as of Visual Studio 2013 Update 2). Support for other languages such as Python,[8] Ruby, Node.js, and M among others is available via language services installed separately. It also supports XML/XSLT, HTML/XHTML, JavaScript and CSS. Java (and J#) were supported in the past. Microsoft provides a free version of Visual Studio called the Community edition that supports plugins and is available at no cost.

## **7. SYSTEM TESTING**

Testing enhances the integrity of a system by identifying deviations in design and development of the expected end product. It should focus more on the error-prone areas of the application. This help in the prevention of errors in a system and builds confidence that the system will work without error after testing. It is the process of executing a program with the intent of finding an error. Testing verifies that software deliverable conforms precisely and design phases. A good test case is one that has a high probability of finding an as yet undiscovered error.

Testing involves a series of operation of a system of application under controlled conditions and subsequently evaluating the result. The controlled condition should include both normal and abnormal conditions. It is planned and monitor for each testing level (example, unit, integration, system and acceptance)

Testing is the major quality measure employed during software development. After the coding phase computer programs are available that can be executed for testing purpose. Testing not only has to uncover errors introduced during coding, but also locates error committed during the previous phase. Thus the aim of testing is to uncover requirements, design or coding errors in the programs

System testing of software is testing conducted on a complete, integrated system to evaluate the system's compliances with its specified requirements. System testing falls within the scope of black box testing and such should require no knowledge of the inner design of the code. As a rule, testing takes as its input, all of the integrated software that have successfully passed integration testing.

Testing is a process of executing a program with interest of finding an error. A good test is one that has high probability of finding the yet undiscovered errors. The primary objective test case design is to drive a set of tests that has highest likelihood for systematically uncovering different class of error in the software. Testing begins at the level and works outward to words the interaction of the entire software. A series of testing are performed for this project before system is ready for acceptance. Some of the testing strategies applied system is listed here.



## Testing Guidelines:

Some of important guide lines for testing the software are given below.

Testers while testing the product must have destructive attitude in order to do effective testing. Testing must start the moment requirement analysis phase starts in order to avoid defective migration. Both functional as well as non-functional requirements of the software must be tested. As far as possible testing must be supported by automated testing tools. Full testing that is, starting from the requirement phase till the acceptance testing must be used for critical software. Testing should also be conducted by a third party independently for effective results. Test were must be properly documented using software test standards and controlled using configuration management system.

## Testing Methods:

Testing is the phase where the bug in the programs was to be found and correct one of the goals during dynamic testing is to produce a test suite, where the salary calculated with the desired outputs such as reports in the case. This is applied to ensure that the modification of the program does not have any side effects. This type of testing called regression testing. Testing generally removes all the residual bugs and improves the bugs and improves the reliability of the program. The basic types of testing are:

- Unit testing
- Integration testing
- Validation testing
- Output testing
- User acceptance testing

## 7.1 UNIT TESTING

Unit test comprises the set of tests performed by an individual programmer prior to integration of unit to large systems.

**Coding & debugging**

**unit testing**

**integration testing**

Unit testing done to testing the modules (classes) one by one in order to make sure that work by themselves before it was put together with other modules. The tests are very simple, at least for small modules with small interfaces to the out world. What was done

to test the classes is to use the different methods that are defined and make sure they return the results that should be expected. Each and every screen was put into testing by giving random values as input. Breakage testing was done with the boundary condition too. The modules were checked to see that the methods return the expected results and that the classes handle the wrong input in a correct way, for example, error messages whenever needed and can handle exception effectively.

## 7.2 INTEGRATION TESTING

Integration testing is the phase in software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing.

The purpose of integration testing is to verify functional, performance and reliability requirements placed on major design items. These “design items” , i.e. assemblies (or groups of units), are exercised through their interfaces using Black box testing, success and error cases being simulated via appropriate parameter and data inputs. Simulated usage of shared data areas and inter-process communication is tested and individually subsystems are exercised through their input interface. Test cases are constructed to test that all components within assemblages interact correctly, for example across procedure calls or process activations, and this is done after testing individual modules, i.e. unit testing. The overall idea is a “building block” approach, in which verified assemblages are added to a verified base which is then used to support the integration testing of

## 7.3 VALIDATION TESTING

It provides the final assurance that the software meets all the functional, behavioral

and performance requirements. The software is completely assembled as a package. Validation succeeds when the software functions in a manner in which the user expects. Validation refers to the process of using software in a live environment in order to find errors.

System validation checks the quality of the software in both simulation and live put a lot of validation testing before finally implementing it. Thus the feedback from the validation phase generally produces changes in the software. The system objective, the functional performance, requirements were looked into see whether all these criteria are satisfying the system needs.

The system is then presented before the manager along with the reports generated the system then undergoes a testing phase with the sample test data provided by him. System testing in this manner would verify that all the modules works together and generate the intended results. All individual modules should be working in tandem so that the overall system function or performance is achieved.

## 7.4 USER ACCEPTANCE TESTING

User acceptance testing is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with prospective system at the time of developing and making changes whenever required. This is done with regarding to the following points. Input screen design, output screen design and menu driven system. It is formal testing conducted to determine whether or not the system satisfies its acceptance criteria to enable the customer to determine whether or not to accept the system. User acceptance of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required. Preparation of data plays a valid role in the system testing after preparing the test data the system under study is tested using the test data. While testing the system by using test data errors are again uncovered and corrected and the corrections are also noted for future use

## **8. CONCLUSION**

The internet applications that make use of the database system face challenges in terms of security and protection of private data . It is important to know how to identify and remediate SQL injection vulnerabilities because the vast majority of data breaches are due to poorly coded web applications. Any code that constructs SQL statements should be reviewed for SQL injection vulnerabilities since a database server will execute all queries that are syntactically valid. Sql Injection Detection And Prevention System provides security by preventing sql injection attacks. This system also further prevents BruteForce attacks and DDos attacks.

## **9. FUTURE ENHANCEMENT**

The proposed system can be updated to support php related attacks, an extension to handle php attacks may be added to the system.It can be further enhanced to deal with dynamic IPs.It is possible that an attacker is able to change IP addresses then our system will not be able to block all the ip addresses that the attacker is able to use.This project would be more effective if it is able to deal with attackers that change their ip addresses.

## **10.REFERENCE**

- <https://pdfs.semanticscholar.org/5239/a6e108226b8264c4275eeacc8787b95019f3.pdf>
- <https://www.codeproject.com/Articles/813965/Preventing-SQL-Injection-Attack-ASP-NET-Part-I>
- <https://security.stackexchange.com/questions/68701/how-does-stored-procedure-prevents-sql-injection>
- "SQL Injection." owasp.org. The Open Web Application Security Project
- "SQL Injection Prevention Cheat Sheet." owasp.org. The Open Web Application Security Project, July 8, 2012. Web. November 8, 2012. "Blind SQL Injection." owasp.org. The Open Web Application Security Project

# APPENDIX

## 11. APPENDIX

### 11.1 SCREENSHOT

#### Home page



#### Registration page

The screenshot shows the Registration page of the application. It features a dark brown background. On the left, there is a vertical navigation menu with three options: HOME, USER REGISTRATION, and LOGIN, each underlined. To the right of the menu, the title "SQL INJECTION AND PREVENTION" is displayed in a large, red, serif font. Below the title, there is a registration form with the following fields and values:

Name	Haneena	UserName	haneena
Sex	<input checked="" type="radio"/> Male <input type="radio"/> Female	Password	*****
Address	16, automobile Road , palarivattom , kochi		
		confirm Password	*****
Mob No	8965713240		
Email	haneena@gmail.com		
<input type="button" value="Register"/>			

At the bottom left, a small text credit reads "Designed by Aksa , Arsha , Sruthi".

### Login page

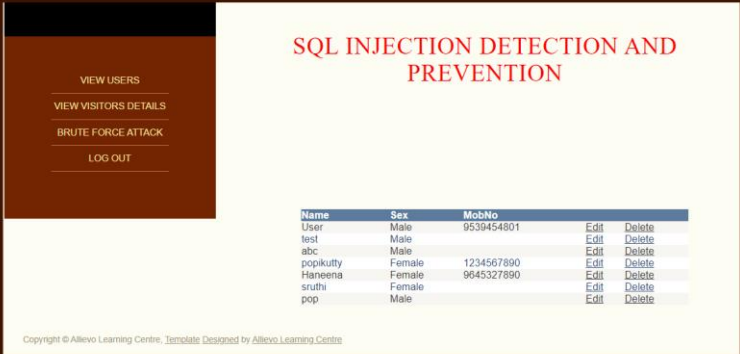
The screenshot shows a web application interface with a dark brown background. On the left, there is a vertical sidebar with a dark brown header and a lighter brown body containing the following links: HOME, USER REGISTRATION, and LOGIN. The main content area has a light cream background. At the top of this area, the title "SQL INJECTION AND PREVENTION" is displayed in red. Below the title, there is a login form with two input fields: "UserName" containing the text "admin@gmail.com" and "Password" containing masked characters "\*\*\*\*\*". A "Login" button is positioned below the password field. At the bottom left of the main content area, a small text credit reads "Designed by Aksha , Anisha , Sruthi".

### Admin home page





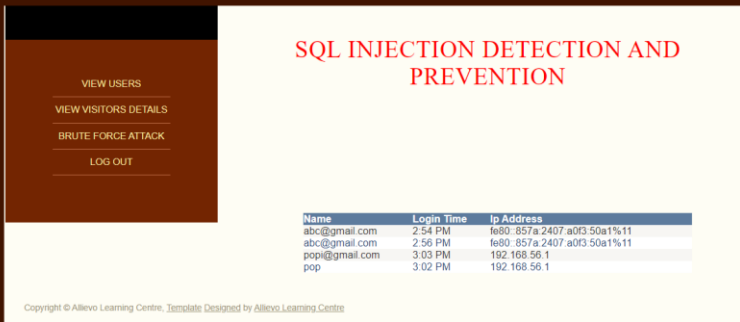
## USERS LIST



Name	Sex	MobNo	Edit	Delete
User	Male	9539454801	Edit	Delete
test	Male		Edit	Delete
abc	Male		Edit	Delete
popikutty	Female	1234567890	Edit	Delete
Haneena	Female	9645327890	Edit	Delete
sruthi	Female		Edit	Delete
pop	Male		Edit	Delete

Copyright © Allievo Learning Centre. Template Designed by Allievo Learning Centre

## VISITORS LIST



Name	Login Time	Ip Address
abc@gmail.com	2:54 PM	fe80:857a:2407:a0d3:50a1%11
abc@gmail.com	2:56 PM	fe80:857a:2407:a0d3:50a1%11
pop@gmail.com	3:03 PM	192.168.56.1
pop	3:02 PM	192.168.56.1

Copyright © Allievo Learning Centre. Template Designed by Allievo Learning Centre

## USER LOGIN

The screenshot shows a web application interface with a dark blue header and a light blue sidebar. The sidebar contains links for HOME, USER REGISTRATION, and LOGIN. The main content area has the title 'SQL INJECTION AND PREVENTION' in red. Below the title, there is a login form with fields for 'UserName' (containing 'haneena@gmail.com') and 'Password' (masked with dots). A 'Login' button is positioned below the password field. At the bottom left, it says 'Designed by Aksha , Arsha , Sruthi'.

SQL INJECTION AND PREVENTION

HOME  
USER REGISTRATION  
LOGIN

UserName haneena@gmail.com  
Password \*\*\*\*\*  
Login

Designed by Aksha , Arsha , Sruthi

## PROFILE

The screenshot shows the same web application interface as the login page. The sidebar now has links for PROFILE and LOG OUT. The main content area has the title 'SQL INJECTION DETECTION AND PREVENTION' in red. Below the title, it displays 'Current IpAddress : 192.168.56.1' in red. A table shows user details: Name (Haneena), Sex (Female), and MobNo (8574963214). An 'Edit' button is next to the table. At the bottom left, it says 'Copyright © Allievo Learning Centre, Template Designed by Allievo Learning Centre'.

SQL INJECTION DETECTION AND PREVENTION

PROFILE  
LOG OUT

Current IpAddress : 192.168.56.1

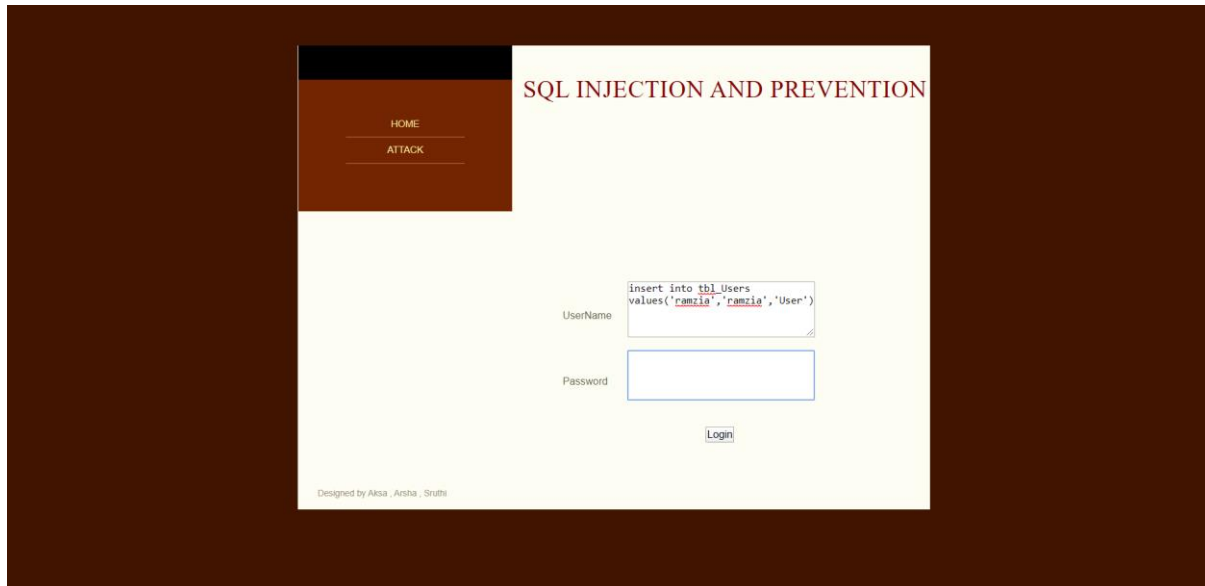
Name	Sex	MobNo	
Haneena	Female	8574963214	Edit

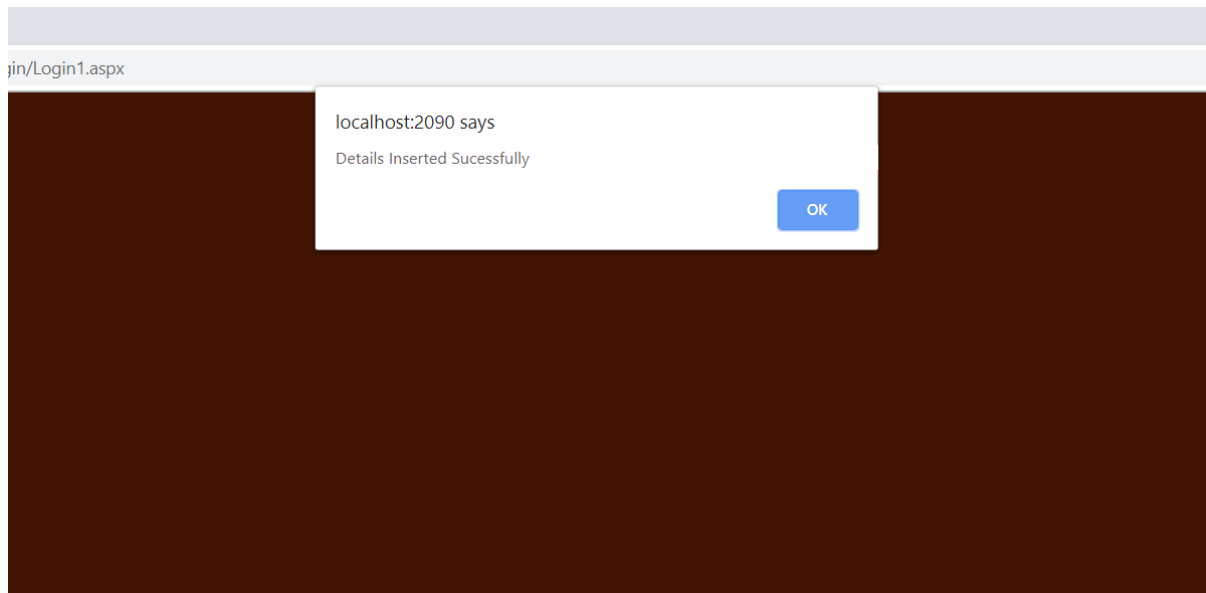
Copyright © Allievo Learning Centre, Template Designed by Allievo Learning Centre

## ATTACK

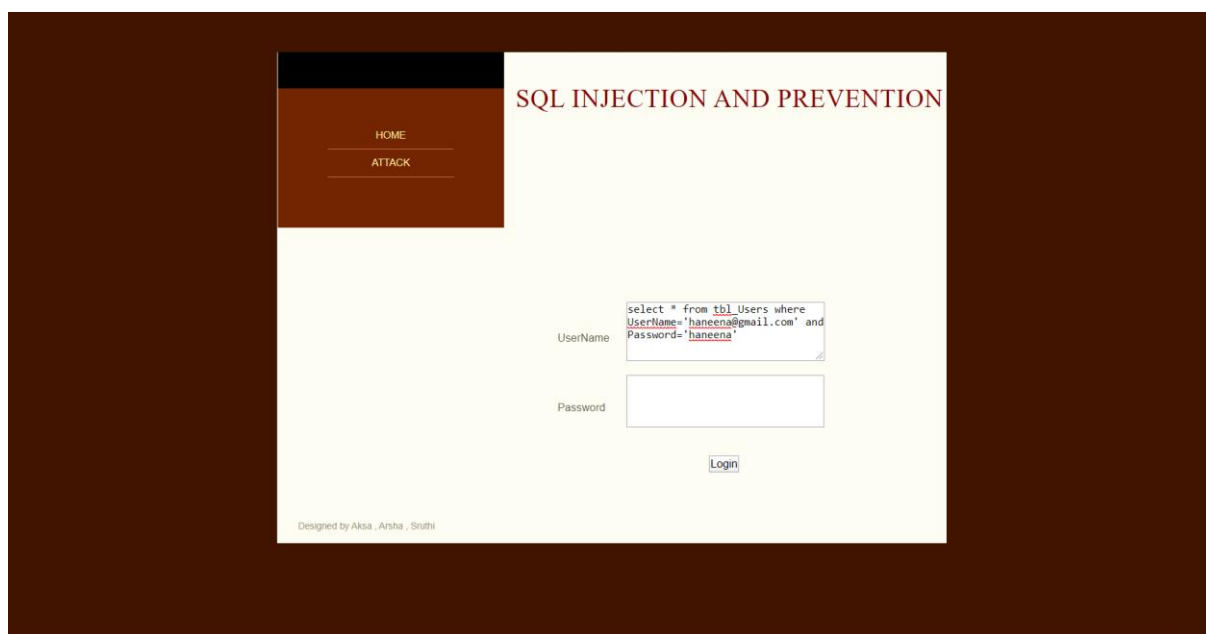


## INSERT QUERY





## SELECT QUERY



## DELETE QUERY

The screenshot shows a web application interface with a dark brown background. On the left, there is a vertical navigation menu with two links: 'HOME' and 'ATTACK'. The main content area has a light yellow background and is titled 'SQL INJECTION AND PREVENTION'. It contains a login form with two input fields: 'UserName' and 'Password'. The 'UserName' field contains the SQL injection payload: `delete from tbl_Users where ID='42'`. Below the input fields is a 'Login' button. At the bottom left of the main content area, it says 'Designed by Aksa , Arsha , Sruthi'.

