FINAL YEAR PROJECT REPORT

SECURING DATA LEAKS VIA SQL INJECTION ON AN E-COMMERCE WEBSITE

In fulfillment of the requirement
For degree of
BS (COMPUTER SCIENCES)

By

ABDUL SAMI	**54177 BSCS**
DAIM ABBAS	**54112 BSCS**
MUHAMMAD MOIN KHAN	**54192 BSCS**

SUPERVISED

BY

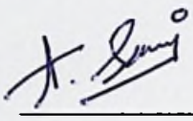
SIR JAWAD BHUTTA

BAHRIA UNIVERSITY (KARACHI CAMPUS)

FALL-2022

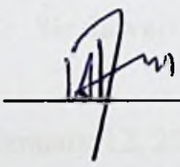
DECLARATION

We hereby declare that this project report is based on our statistical work approach aside from the citations and quotations which have been duly acknowledged. We also claim that it has not been previously and concurrently submitted for any other degree or award at Bahria University or other institutions.

Signature : 

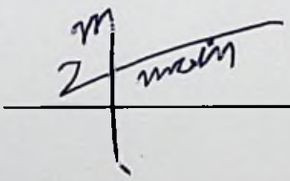
Name : **ABDUL SAMI**

Reg No. : 54177

Signature : 

Name : **DAIM ABBAS**

Reg No. : 54112

Signature : 

Name : **MUHAMMAD MOIN KHAN**

Reg No. : 54192

Date : 1/2/2022

The copyright of this report belongs to Bahria University according to the Intellectual Property Policy of Bahria University BUORIC-P15 amended in April 2019. Due acknowledgement shall always be made of the use of any material contained in, or derived from, this report.

© 2021 Bahria University. All right reserved.

Specially dedicated to

my beloved grandmother, mother and father

(ABDUL SAMI)

my beloved grandmother, mother and father

(DAIM ABBAS)

my beloved grandmother, mother and father

(MUHAMMAD MOIN KHAN)

ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express my gratitude to my research supervisor, **SIR JAWAD BHUTTA** for his invaluable advice, guidance, and his/her enormous patience throughout the development of the research.

In addition, we would also like to express my gratitude to our loving parent and friends who had helped and given me encouragement.

SECURING DATA LEAKS VIA SQL INJECTION ON AN E-COMMERCE WEBSITE

ABSTRACT

Nowadays e-commerce websites are very popular for online shopping in this pandemic. While in this digital world the online security breach is a big threat to the real world as it can be very dangerous for a person or any organization who get attacked by these hackers. A lot of users get cash out of their Credit Cards while ordering online and they get access of user details. Even though technology has advanced significantly in recent years, hackers can still exploit security flaws to do SQL injections. Hackers can use a variety of methods to accomplish SQL injections, and there are numerous ways to prevent SQL injections from occurring. The vulnerability to SQL injections is significant and it pose a significant threat to web based applications since hackers may quickly enter their system and access whatever data and information they choose, at any time and from any location. The project is based on the prevention of **SQL injection Queries via secured Database and AES.**

TABLE OF CONTENTS

DECLARATION		**2**
APPROVAL FOR SUBMISSION		**3**
ACKNOWLEDGEMENTS		**6**
ABSTRACT		**7**
TABLE OF CONTENTS		**8-10**
LIST OF TABLES		**11**
LIST OF FIGURES		**12**
CHAPTER'S		
1	**INTRODUCTION**	**13-15**
	1.1 Background	13-14
	1.2 Problem Statements	14
	1.3 Aims and Objectives	14-15
	1.4 Scope of Project	15
2	**LITERATURE REVIEW**	**17-21**
	2.1 Sql Injection Implementation/Prevention	16-17
	2.2 E-Commerce Web Development	17-18
	2.2.1 Php Scripting Language	17
	2.2.2 Mysql Database, Js, Css & Html	17-18
	2.3 Sql Injection Implementation/Prevention	18-20
3	**DESIGN AND METHODOLOGY**	**22-29**
	3.1 Design	22

	3.1.1	System Block Diagram	22-23
	3.1.2	Tools & Languages	23
	3.1.3	Design of the study	23
3.2	Project Methodology		24
3.3	Modules		24-25
	3.3.1	Admin Login	25
	3.3.2	User login & Registration	25
	3.3.3	MySQL DataBase	25
3.4	Workflow of The Project		25-26
3.5	Sql Injections & its Types		26-27
	3.5.1	In-Band SQLI	27
	3.5.2	Infarantial (Blind) SQLI	27
	3.5.3	Out-Of-Band SQLI	27
3.6	AES (Advanced Encryption System)		29
4	**IMPLEMENTATION**		**30-46**
4.1	Installation of Web Server		30
4.2	Creating Structure		30
4.3	Adding Additional Features		31-36
4.4	Admin Portal Overhaul		36-40
4.5	Customer Product Selection & Payment		40-41
4.6	Database Connectivity		41
4.7	Basic Input Validation Check		41
4.8	Parameterization		41-43
4.9	Encryption Scheme		43-44
4.10	Additional Measures		44-46
5	**RESULT & TESTING**		**47-53**