

Acknowledgement

I would like to avail this opportunity to thank all of the people who have stood by me in, encouraged me, inspired me and have contributed greatly in providing me with the joy of achievement and thrill of creative effort experienced by me all the way through the accomplishment of my Internship.

It's my greatest privilege to express gratitude to my guide **Miss. Keerthi Ramji, B.E Lecturer** Computer Science and Engineering Department for her constant presence and valuable advice has led to the completion of this Internship.

I wish to express my sincere thanks to **Mrs. Archana S. Hinchigeri, Head Of** Department, Computer Science and Engineering Department for her valuable suggestions, help and support.

I sincerely thank Prof. **Veeresh B. Angadi**, Principal of **K.L.E's SMT. C.I Munavalli Polytechnic, Hubli** for the support he has provided in permitting me to undertake this Internship.

We also acknowledge our gratitude to all the staff member of the **Computer Science and Engineering Department, K.L.E's SMT C. I. Munavalli Polytechnic, Hubli** who have extended their moral support during the course of the Internship.

Finally, we wish to express thanks to our parents, friends and regards to one and all who have helped us directly or indirectly in the internship.

EXECUTIVE SUMMARY

SQL injection is a prevalent and potentially devastating cybersecurity threat that targets web applications by exploiting vulnerabilities in SQL database queries, to safeguard against this threat, effective prevention and detection measures are essential.

Prevention Measures:

- **Input Validation:** Implement strict input validation mechanisms to ensure that user-supplied data is sanitized and adheres to expected formats. This prevents malicious input from being executed as part of SQL queries.
- **Parameterized Queries:** Utilize parameterized queries or prepared statements to separate SQL code from user input. By treating user input as data rather than executable code, the risk of SQL injection attacks is significantly reduced.

Detection Measures:

- **SQL Injection Signatures:** Clinic Management system that utilize signature-based detection techniques to identify known pattern and signatures associated with SQL injection attacks.
- **Anomaly Detection:** Implement anomaly detection algorithms that analyze SQL query patterns and user behavior to detect deviations indicative of SQL injection attacks, such as unusually long or complex queries.
- **Database Activity Monitoring (DAM):** Utilize DAM solutions to monitor and analyze database activity in real-time, enabling the detection of suspicious SQL injection-related activities, such as unauthorized access attempts or abnormal query execution.

CONTENTS

Acknowledgement	I
Executive Summary	II
Contents	III
List of Figures	IV
Abbreviations	VII
CHAPTER 1	
1.1 Overview of the organization	
1.1.1 HA EGL	1-2
1.1.2 HA EGL Cloud Excellence	2
1.1.3 Grants Received	2
1.2 Vision and Mission of the Organization	
1.2.1 HA EGL Vision	3
1.2.2 HA EGL Mission	3-4
1.2.3 Key Strategies	4
1.3 Organization Structure	5
1.4 Roles and Responsibilities of Personnel in the Organization	
1.4.1 Founder	6
1.4.2 The Chief operating Officer (COO)	6
1.4.3 The Chief Technology Officer (CTO)	6
1.4.4 Software Development	7
1.4.5 Manager	7
1.4.6 IOT Engineer	8
1.5 Products and Market Performance	
1.5.1 Key feature	9
1.5.2 HA EGL offerings	10-11
1.5.3 HA EGL Pioneering Discoveries	11
1.5.3.1 HA EGL Hybrid Solar Tunnel Dryer	11-12

CHAPTER 2

2.1 Introduction

2.1.1 Cybersecurity	13-14
---------------------	-------

2.2 Advantages of Cybersecurity	15
---------------------------------	----

2.3 Disadvantages of Cybersecurity	15
------------------------------------	----

2.4 Different types of attacks in Cybersecurity

2.4.1 Overview of the attacks

2.4.1.1 SQL Injection	16-17
-----------------------	-------

2.4.1.2 Broken Authentication	17-18
-------------------------------	-------

2.4.1.3 Brute Force	18-19
---------------------	-------

2.5 Literature Survey

2.5.1 SQL Injection	20-21
---------------------	-------

2.5.2 Broken Authentication	21-22
-----------------------------	-------

2.5.3 Brute Force	22-23
-------------------	-------

2.6 System Specification

2.6.1 Hardware Specification	24
------------------------------	----

2.6.2 Software Specification	24
------------------------------	----

2.7 Development Tools

2.7.1 Frontend	25
----------------	----

2.7.2 Backend	25
---------------	----

2.7.3 Database	25
----------------	----

2.8 Design

2.8.1 ER diagram for Clinic Management System	26
---	----

2.8.2 Architectural Diagram of the website	27-29
--	-------

2.8.3 Class Diagram	30
---------------------	----

CHAPTER 3

3.1 Implementation

3.1.1 SQL Injection	31-34
---------------------	-------

3.1.2 Broken Authentication	35-40
-----------------------------	-------

Clinic Management System	2024-2025
3.1.3 Brute Force	41-44
3.2 Prevention of Attacks	45-46
CHAPTER 4	
4.1 UML-Building Block	46-51
4.2 Diagrams	51-52
4.3 Conclusion	53
RESUME	54
Photo Gallery	55
Appendices	56

LIST OF FIGURES

Figure Number	Figure Name	Page Number
Figure 1.1	Structure of the organization	5
Figure 1.2	Talent sourcing strategy for the year-2024	5
Figure 1.3	Hybrid Solar Tunnel Dryer	11
Figure 2.1	Cybersecurity	13
Figure 2.2	Function of SQL Injection	16
Figure 2.3	Function of Broken Authentication	17
Figure 2.4	Brute Force	18
Figure 2.5	Function of Broken Authentication	21
Figure 2.8.1	ER-diagram For Clinic Management System	26
Figure 2.8.3	Class Diagram	30
Figure 3.1.1	Implementation of SQL Injection	31
Figure 3.1.2	Implementation of Broken Authentication	35
Figure 3.1.3	Implementation of Brute Force	41
Figure 4.1	Interface	47
Figure 4.2	Collaboration	47
Figure 4.3	Use Case	48
Figure 4.4	Actor	48
Figure 4.5	Component	48
Figure 4.6	System Components	49

Abbreviations

SQL: Structured Query Language
UML: Unified Modelling Language
SDLC: Software Development Life Cycle
VM: Virtual Machine
COO: Chief Operating Officer
CTO: Chief Technology Officer
IOT: Internet of Things
CRM: Customer relationship management
ERP: Enterprise resource planning
IDS: Intrusion Detection System
VPN: Virtual private network
DoS: Denial-of-Service
EDR: Endpoint detection and response
2FA: Two-factor authentication
MFA: Multi-factor authentication
RAM: Random access memory
ER: Entity–relationship
URL: Uniform Resource Locator
HTTPS: Hypertext Transfer Protocol Secure
RBAC: Role-based access control
XSS: Cross-Site Scripting