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 form being executed as part of SQL queries.
- Parameterized Queries: Utilize parameterized queries or prepared statements to separate SQL code form user input. By treating user input as data rather then 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 SQI. 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-tune, enabling the detection of suspicious SQL injection-related activities, such as unauthorized access attempts or abnormal query execution.

CONTENTS

LIST OF FIGURES

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