



Securing Data Integrity Advanced Techniques for Detecting and Mitigating SQL Injection Threats

Princy Ruth S¹, Dr. Vaidehi V²

¹PG Student, ²Professor

Department of Computer Applications, Dr. M.G.R Educational and Research Institute, Chennai-600095.

Email: princyruth18@gmail.com¹ vaidehi.mca@drmgrdu.ac.in²

ABSTRACT:

Third-party file injections pose a significant threat to the security of web applications, potentially leading to data breaches, unauthorized access, and compromised sensitive information. The primary objective of this study is to develop proactive strategies and mitigation techniques to safeguard web applications against file injection vulnerabilities introduced by third-party entities. This research methodology involves a comprehensive analysis of common third-party file injection attack vectors, including those that exploit dependencies, libraries, and external resources. A systematic examination of coding practices, input validation mechanisms, and security protocols was conducted to identify the potential vulnerabilities. This study also explored the use of static and dynamic code analysis tools to enhance the detection of injection points. Building upon the identified vulnerabilities, this study proposes and implements defense mechanisms, including input validation, code sanitization, and the implementation of Content Security Policy (CSP) directives. The effectiveness of these defense mechanisms was evaluated using penetration testing and simulated attack scenarios.

KEYWORDS: SQL injection, database security, anomaly detection, , detection, and prevention

I. INTRODUCTION

SQL injection is a type of database threat used to breach websites and gain access to underlying databases. These attacks are launched to access databases containing sensitive data by exploiting security vulnerabilities on websites. This attack is particularly concerning because it can bypass various security layers, such as encryption and firewalls, exploiting weaknesses in input validation. SQL injection attacks can easily circumvent database defenses [1].

This attack is relatively straightforward and can be executed with minimal effort, often by exploiting webpages that lack the proper validation of user inputs. During the login and authentication processes, users typically provide their usernames and passwords for verification. However, if these inputs are not properly validated, they can be manipulated to form malicious SQL statements, thereby enabling SQL injection attacks [2].

SQL is a query-based scripting language that allows users to interact with databases. SQL injection attacks can provide unauthorized access to database servers. In such attacks, the client's input is interpreted as SQL code, potentially allowing them to access the database through scripting languages, such as JAVA, by issuing fundamental queries. When user-provided data are sent directly to the database without proper validation, it creates a vulnerability that can be exploited by inserting malicious SQL code [3].

Attackers can then execute SQL queries directly in the database, leading to data exploitation. For instance, they may execute change or delete queries, rendering data irrecoverable and inaccessible. In more severe cases, attackers can execute remote code, granting them access to data stored in the database

II. LITERATURE SURVEY

Nanang Cahyadi .et al.,2023 literature suggests comprehensive resilience requires concurrent strengths in these areas. Finally, destiny paintings remain in incorporated frameworks, deep reinforcement learning adoption, automated AI auditing, and differential privacy to advance Real-world SQL injection detection and prevention methods [5].

Md. Hasan Furhad .et al., 2022 a hybrid method is proposed that combines a SQL query Matching technique (SQLMT) and a fashionable blockchain framework to stumble on SQL attacks created by insiders. The results obtained using the proposed hybrid approach via computational experiments were further validated using standard web validation tools [6].

Kamsuriah Ahmad.et al., 2021 Experimental results prove that the proposed method is able to save you SQL injection from happening and capable of shorten the processing time while compared with existing methods, hence able to improve database security [7].

Kirti Sharma .et al., 2019 This research paper starts with developing criteria for systematic Literature evaluate primarily based totally on studies questions, first-class evaluation and information samples. This paper presented numerous SQL injection strategies based on their supposed attacks. Further research is required to discover unique strategies to protect against such attacks. A tabular illustration of the best assessment standards is presented in the grades. Finally, one of a kind studies questions and answers have been supplied related to SQL injection attacks are provided [8].

Sadotra et al., 2017 SQL Injection Impact on Web Server and Their Risk Mitigation Policy Implementation Techniques: An Ultimate way to prevent Computer Network from illegal Intrusion [9].

Chandrakant .et.al.,2017 many answers proposed in the literature address only a few of the problems associated with SQL injection. To address this problem, we provide an extensive review of specific forms of SQL injection assaults acknowledged to date. Also for every form of attack, we provide descriptions and examples of how attacks of that type could be performed[10]

III. PROPOSED SYSTEM:

The proposed system is robust and easy to deploy. During the complete procedure of protection code encryption and decryption, the document on the nodes no longer gets crashed. SQL injection assaults interactive net packages that offer database services. These applications take user input and use it to create an SQL query at the runtime. In an SQL injection attack, an attacker can insert a malicious SQL question to perform an unauthorized database operation. Using SQL injection attacks, an attacker can retrieve or regulate private and touchy statistics from the database

ARCHITECTURE DIAGRAM

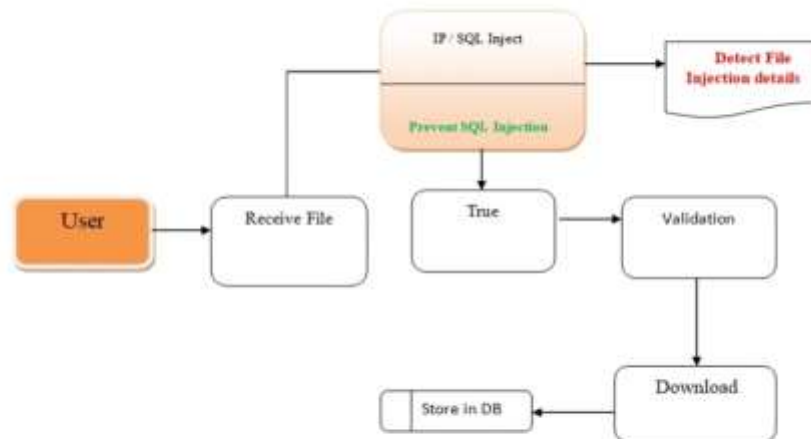


Fig 1: Architecture of proposed system

EXPLANATION:

Fig 1 shows the architecture of the proposed system. This system allows the admin, provider, and user to log in through credentials. After logging successfully, the admin performs the monitoring tasks. This includes tracking the number of files uploaded, total number of users, and viewing user activity history. admin performed monitoring tasks.

MODULE DESCRIPTION

System improvement offers operations that might be accomplished to obtain favored output from software program products primarily based entirely on certain layout specifications. This Application holds the following modules.

1. ADMIN
2. PROVIDER
3. USER

1. ADMIN :

The Admin Dashboard and Management module serves as the central hub for system administrators to oversee and manage various aspects of the platform. Administrators can access real-time analytics, monitor user activities, and configure the system settings to ensure optimal performance and security. Key functionalities include user management, role-based access control, system configuration, and monitoring tools. This module provides a user-friendly interface with intuitive navigation, enabling administrators to manage resources efficiently, resolve issues, and maintain data integrity across platforms.

2. PROVIDER :

Upon successfully logging into as a provider, users can execute a range of tasks. For example, they can upload files using AES encryption, distribute the files to other users, verify the status of their files, and oversee user requests related to the file in question.

3.USER :

The user module involves account registration and a subsequent login to perform operations. Once logged in, users can view file details, request access to files, and download files. If an unauthorized user attempts to tamper with the files, the system automatically logs and shares the IP address and details with the administrator. Each module serves a specific role within the system, with admin overseeing and managing overall activities, providers handling file-related operations, and users interacting with and securely accessing the files. The system includes security measures such as AES encryption for file uploads and automated logging of suspicious activities to protect against unauthorized access or tampering.

IV. RESULT AND DISCUSSION



FIGURE.2 Home Page

Homepage design and layout effectively engage users, encouraging platform exploration and interaction. Continuous monitoring and optimization enhance usability and user retention.



FIG.3 Admin Login Page

Admin Login Page features robust authentication and encryption mechanisms, ensuring secure access to administrators. Iterative development and user feedback streamlined this logical process.

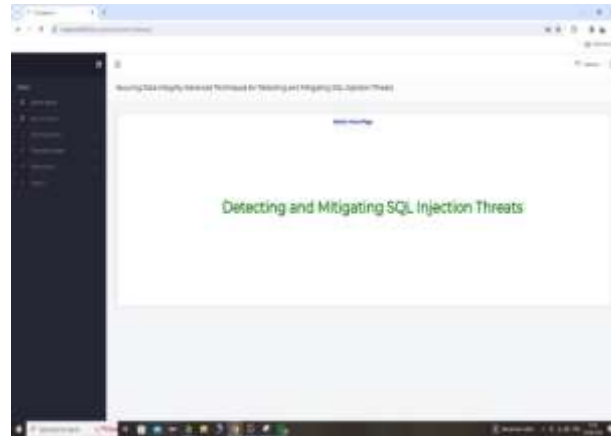


FIG.4 Admin Home Page

The Admin Home Page offers a centralized dashboard with real-time data visualization and reporting tools. Ongoing enhancements based on user feedback optimize administrative efficiency.

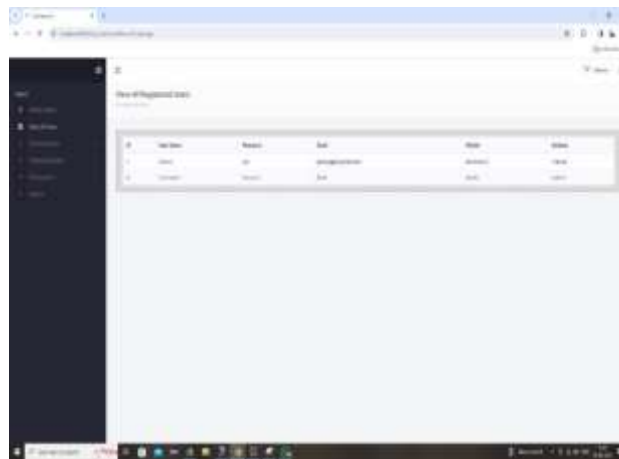


FIG.5 View All Users

The View All Users feature provides administrators with a comprehensive overview of the management capabilities for user profiles. The efficient handling of large datasets and user feedback provided continuous improvements.

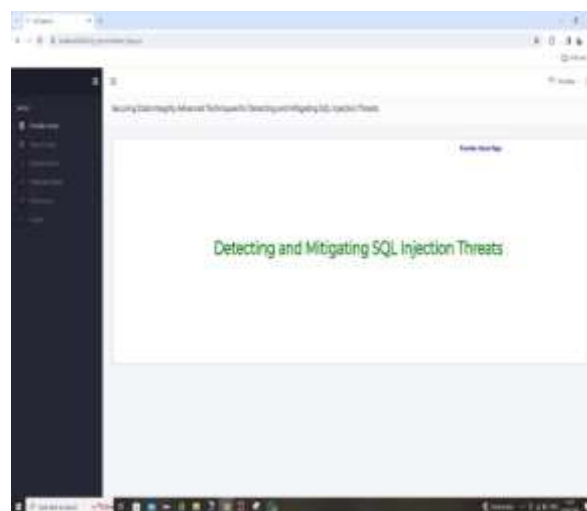


FIG.6 Provider Home Page

Our homepage redesign offers a clear overview of our services, emphasizing the key features and benefits through strategic layouts and engaging visuals. The user-friendly design ensures seamless navigation across devices with a focus on accessibility and responsiveness.

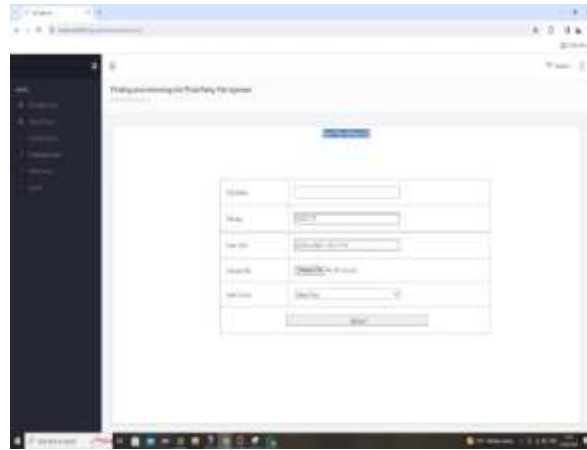


FIG.7 Send File without AES

The Send File functionality enables secure file sharing within a platform by utilizing encryption methods other than the AES. Testing ensured the integrity and confidentiality of the data.

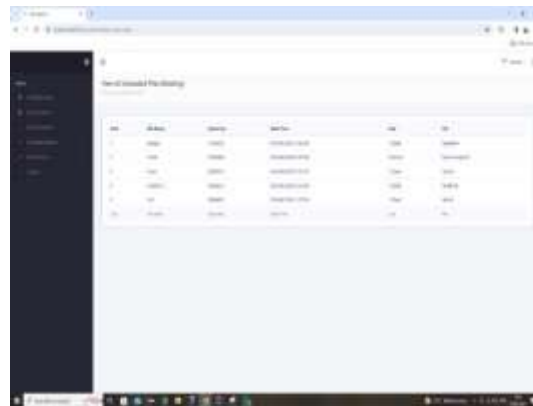


FIG.8 View Upload File

The View Upload File feature allows users to access and review uploaded files. User-friendly interfaces and efficient data retrieval enhance the user experience and accessibility.

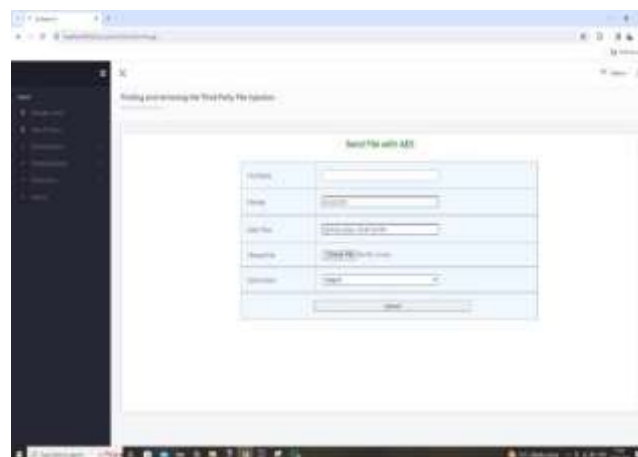
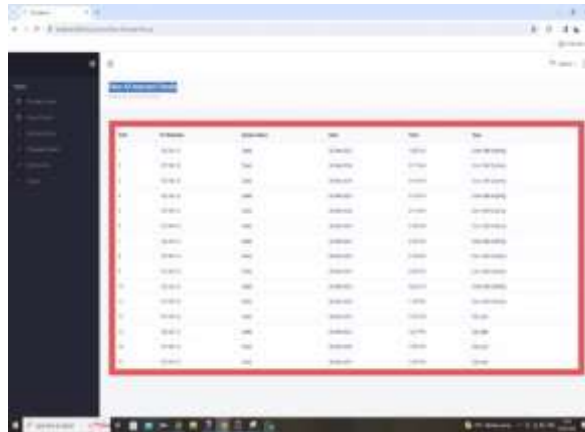


FIG.9 Send File with AES

The end file with AES functionality offers enhanced security through the encryption and safeguarding of file transfers. Thorough testing validated the integrity and effectiveness of the AES encryption.



ID	Username	Password	Email	Phone	Address
1	admin	admin	admin@admin.com	08123456789	Jakarta
2	user1	user1	user1@user1.com	08123456789	Jakarta
3	user2	user2	user2@user2.com	08123456789	Jakarta
4	user3	user3	user3@user3.com	08123456789	Jakarta
5	user4	user4	user4@user4.com	08123456789	Jakarta
6	user5	user5	user5@user5.com	08123456789	Jakarta
7	user6	user6	user6@user6.com	08123456789	Jakarta
8	user7	user7	user7@user7.com	08123456789	Jakarta
9	user8	user8	user8@user8.com	08123456789	Jakarta
10	user9	user9	user9@user9.com	08123456789	Jakarta
11	user10	user10	user10@user10.com	08123456789	Jakarta
12	user11	user11	user11@user11.com	08123456789	Jakarta
13	user12	user12	user12@user12.com	08123456789	Jakarta
14	user13	user13	user13@user13.com	08123456789	Jakarta
15	user14	user14	user14@user14.com	08123456789	Jakarta
16	user15	user15	user15@user15.com	08123456789	Jakarta
17	user16	user16	user16@user16.com	08123456789	Jakarta
18	user17	user17	user17@user17.com	08123456789	Jakarta
19	user18	user18	user18@user18.com	08123456789	Jakarta
20	user19	user19	user19@user19.com	08123456789	Jakarta
21	user20	user20	user20@user20.com	08123456789	Jakarta
22	user21	user21	user21@user21.com	08123456789	Jakarta
23	user22	user22	user22@user22.com	08123456789	Jakarta
24	user23	user23	user23@user23.com	08123456789	Jakarta
25	user24	user24	user24@user24.com	08123456789	Jakarta
26	user25	user25	user25@user25.com	08123456789	Jakarta
27	user26	user26	user26@user26.com	08123456789	Jakarta
28	user27	user27	user27@user27.com	08123456789	Jakarta
29	user28	user28	user28@user28.com	08123456789	Jakarta
30	user29	user29	user29@user29.com	08123456789	Jakarta
31	user30	user30	user30@user30.com	08123456789	Jakarta
32	user31	user31	user31@user31.com	08123456789	Jakarta
33	user32	user32	user32@user32.com	08123456789	Jakarta
34	user33	user33	user33@user33.com	08123456789	Jakarta
35	user34	user34	user34@user34.com	08123456789	Jakarta
36	user35	user35	user35@user35.com	08123456789	Jakarta
37	user36	user36	user36@user36.com	08123456789	Jakarta
38	user37	user37	user37@user37.com	08123456789	Jakarta
39	user38	user38	user38@user38.com	08123456789	Jakarta
40	user39	user39	user39@user39.com	08123456789	Jakarta
41	user40	user40	user40@user40.com	08123456789	Jakarta
42	user41	user41	user41@user41.com	08123456789	Jakarta
43	user42	user42	user42@user42.com	08123456789	Jakarta
44	user43	user43	user43@user43.com	08123456789	Jakarta
45	user44	user44	user44@user44.com	08123456789	Jakarta
46	user45	user45	user45@user45.com	08123456789	Jakarta
47	user46	user46	user46@user46.com	08123456789	Jakarta
48	user47	user47	user47@user47.com	08123456789	Jakarta
49	user48	user48	user48@user48.com	08123456789	Jakarta
50	user49	user49	user49@user49.com	08123456789	Jakarta
51	user50	user50	user50@user50.com	08123456789	Jakarta
52	user51	user51	user51@user51.com	08123456789	Jakarta
53	user52	user52	user52@user52.com	08123456789	Jakarta
54	user53	user53	user53@user53.com	08123456789	Jakarta
55	user54	user54	user54@user54.com	08123456789	Jakarta
56	user55	user55	user55@user55.com	08123456789	Jakarta
57	user56	user56	user56@user56.com	08123456789	Jakarta
58	user57	user57	user57@user57.com	08123456789	Jakarta
59	user58	user58	user58@user58.com	08123456789	Jakarta
60	user59	user59	user59@user59.com	08123456789	Jakarta
61	user60	user60	user60@user60.com	08123456789	Jakarta
62	user61	user61	user61@user61.com	08123456789	Jakarta
63	user62	user62	user62@user62.com	08123456789	Jakarta
64	user63	user63	user63@user63.com	08123456789	Jakarta
65	user64	user64	user64@user64.com	08123456789	Jakarta
66	user65	user65	user65@user65.com	08123456789	Jakarta
67	user66	user66	user66@user66.com	08123456789	Jakarta
68	user67	user67	user67@user67.com	08123456789	Jakarta
69	user68	user68	user68@user68.com	08123456789	Jakarta
70	user69	user69	user69@user69.com	08123456789	Jakarta
71	user70	user70	user70@user70.com	08123456789	Jakarta
72	user71	user71	user71@user71.com	08123456789	Jakarta
73	user72	user72	user72@user72.com	08123456789	Jakarta
74	user73	user73	user73@user73.com	08123456789	Jakarta
75	user74	user74	user74@user74.com	08123456789	Jakarta
76	user75	user75	user75@user75.com	08123456789	Jakarta
77	user76	user76	user76@user76.com	08123456789	Jakarta
78	user77	user77	user77@user77.com	08123456789	Jakarta
79	user78	user78	user78@user78.com	08123456789	Jakarta
80	user79	user79	user79@user79.com	08123456789	Jakarta
81	user80	user80	user80@user80.com	08123456789	Jakarta
82	user81	user81	user81@user81.com	08123456789	Jakarta
83	user82	user82	user82@user82.com	08123456789	Jakarta
84	user83	user83	user83@user83.com	08123456789	Jakarta
85	user84	user84	user84@user84.com	08123456789	Jakarta
86	user85	user85	user85@user85.com	08123456789	Jakarta
87	user86	user86	user86@user86.com	08123456789	Jakarta
88	user87	user87	user87@user87.com	08123456789	Jakarta
89	user88	user88	user88@user88.com	08123456789	Jakarta
90	user89	user89	user89@user89.com	08123456789	Jakarta
91	user90	user90	user90@user90.com	08123456789	Jakarta
92	user91	user91	user91@user91.com	08123456789	Jakarta
93	user92	user92	user92@user92.com	08123456789	Jakarta
94	user93	user93	user93@user93.com	08123456789	Jakarta
95	user94	user94	user94@user94.com	08123456789	Jakarta
96	user95	user95	user95@user95.com	08123456789	Jakarta
97	user96	user96	user96@user96.com	08123456789	Jakarta
98	user97	user97	user97@user97.com	08123456789	Jakarta
99	user98	user98	user98@user98.com	08123456789	Jakarta
100	user99	user99	user99@user99.com	08123456789	Jakarta
101	user100	user100	user100@user100.com	08123456789	Jakarta

FIG.10 View All Attacked Details

The View All Attacked Details feature provides administrators with insights into security incidents and breaches. Comprehensive logging and monitoring capabilities aid threat detection and mitigation.

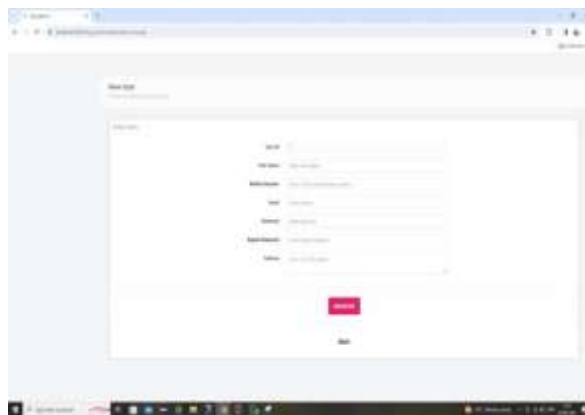


FIG.11 User Register Page

Registration shape is a listing of the fields that a consumer enters and publishes statistics to an individual. There are many reasons why you need someone to complete a registration form. Companies use registration paperwork to join clients through subscriptions, services, or different packages or plans.

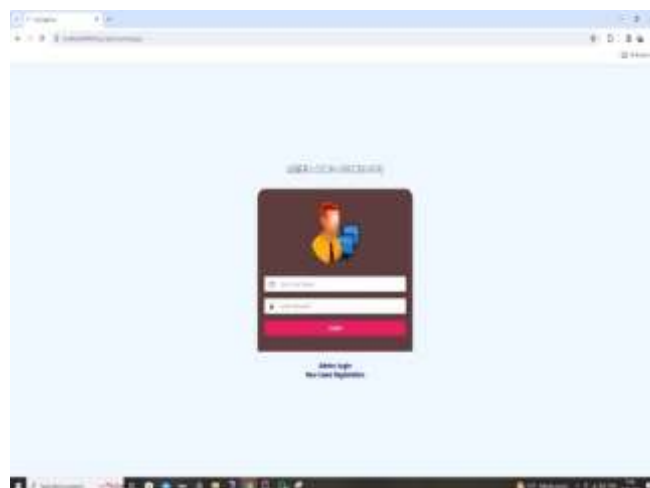


FIG.12 Login Page

Logins are used on websites, PC applications, and cell applications. They are a safety degree designed to save you unauthorized from admission to exclusive data. When a login attempt is unsuccessful owing to an incorrect combination of username and password that does not match a valid account, the user is denied access. Many structures prevent customers from looking to log in after a few failed login attempts.

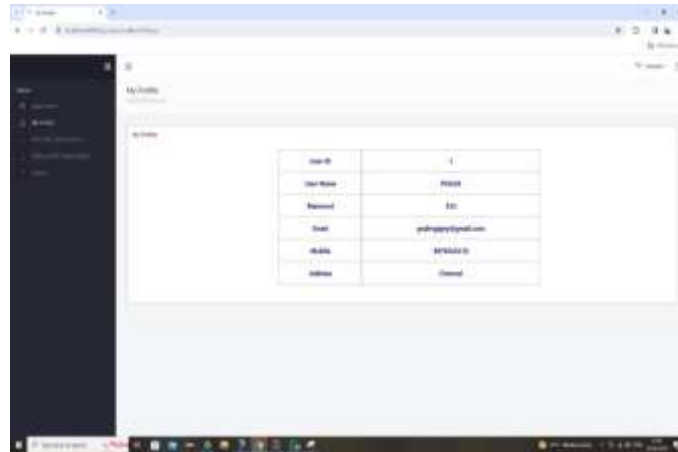


FIG.13 My Profile Page

The My Profile Page allows users to manage and personalize their account settings and preferences. User-centric design and customization options enhance user engagement and satisfaction.

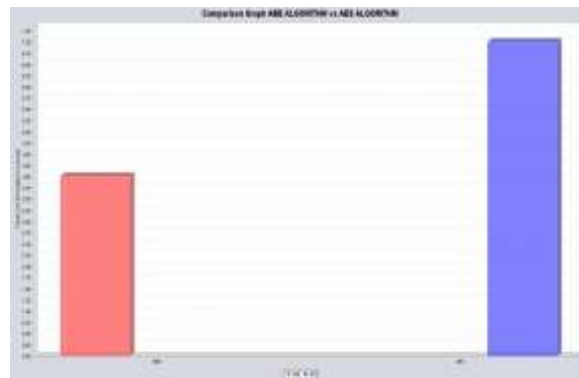


FIG.14 Output Page without AES

The Output Page provides a platform for presenting and analyzing data without requiring AES encryption. This page offers convenient tools for processing and visualizing data, making knowledgeable choices, and interacting with significant interactions.

CONCLUSION:

Throughout this research paper, we have discussed SQL injection as a substantial topic that has been continuously expanding and progressing. This weakness captures the interests of all sectors of data security, and there is no sign of any comprehensive solution emerging in this area. This issue will continue to be a significant concern for years, and individuals who are developing software or systems must be mindful of the potential risks of sensitive data.

Careful attention must be paid to user input when creating software, including ensuring that freeform text is handled with care, and that any system that processes data performs thorough cleansing and validation before use. In addition to handling data with care, it is important to monitor and respond to security vulnerabilities throughout the organization.

V. Reference:

- [1] A. Jamil and Zawiyah Mohammad Yusof, Information Security Governance Framework of Malaysia Public Sector, *Asia-Pacific Journal of Information Technology and Multimedia*, Vol. 7 no. 2, 2018, pp.85 – 98.
- [2] L. Ma, D. Zhao, Y. Gao and C. Zhao, Research on SQL Injection Attack and Prevention Technology Based on Web”, *International Conference on Computer Network, Electronic and Automation (ICCNEA)*, Xi’an, China, 2019, pp. 176-179.
- [3] N. Singh, M. Dayal, R. S. Raw and S. Kumar, “SQL injection: Types, methodology, attack queries and prevention,” *3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2016, pp. 2872-2876.
- [4] Z. C. S. S. Hlaing and M. Khaing, “A Detection and Prevention Technique on SQL Injection Attacks”, *IEEE Conference on Computer Applications (ICCA)*, Yangon, Myanmar, 2020, pp. 1-6.

-
- [5] H. Gaikwad, Bhavesh B. Shah and Priyanka Chatte, —SQLi and XSS Attack Introduction and Prevention Techniquel, International Journal of Computer Applications (0975 – 8887) May 2017 volume 165 – No.2, 23-27. Richa Pokhrel, Asmita Jha , Pooja Singh and Pragya Jha, and Rama Bastola (2020) “Women Self-Defense and Security System”. Volume 3.
- [6] A.Jumaa and Omar, A.. —Online Database Intrusion Detection System Based on Query Signaturesl, Journal of University of Human Development, 3(1), 2017, pp.282–287.
- [7] Sharma, K. and Bhatt, S., 2019. SQL injection attacks: a systematic review. International Journal of Information and Computer Security, 11(4-5), pp.493-509.
- [8] Kirti Sharma . SQL Injection Attacks. Vol. 11, No. 4-5.
- [9] Sadotra, P., & Sharma, C. (2017). SQL injection affects web servers and their risk mitigation policy implementation techniques 8(3).
- [10] Chandrakant, a type of SQL injection assault, has been acknowledged. For each type of attack, we provide descriptions and examples of how attacks of this type can be performed, 2017, Vol. 8, Issue 3. In addition, for each type of attack, we provide descriptions and examples of how attacks of that type could be performed, 2017, Vol. 8, Issue 3.
- [11] O.C. Abikoye, Abubakar, A., Dokoro, A.H. et al. —A novel technique to prevent SQL injection and cross-site scripting attacks using the KnuthMorris-Pratt string-match algorithml, EURASIP J. Info. Security, 2020, 14.
- [12] K.G. Vamshi, V. Trinadh, S. Soundabaya, and A. Omar, —Advanced Automated SQL Injection Attacks and Defensive Mechanismsl, in Annual Connecticut Conference on Industrial Electronics, Technology & Automation (CT-IETA), 2016, p. 1-6.
- [13] M.Amin Mohd Yunus, Muhammad Zainulariff Brohan and Nazri Mohd Nawi. Review of SQL Injection: Problems and Prevention International Journal on Informatics Visualization, vol 2, 2018, No 3 –2.