

**INTRUSION HUNTER**

# PYTHON MINI PROJECT

***Submitted by***

# KRISHNA PARESH RAICHURA [22AM021]

**SREEJHA.J [22AM050]**

**VISHNUPARGAVAN.V [22AM063]**

**BACHELOR OF ENGINEERING IN**

**COMPUTER SCIENCE AND ENGINEERING**

**with specialization in**

# [ARTIFICIAL INTELLIGENCE & MACHINE LEARNING]

**SRI ESHWAR COLLEGE OF ENGINEERING**

**(AN AUTONOMOUS INSTITUTION)**

**COIMBATORE – 641 202**

**JULY 2023**

# BONAFIDE CERTIFICATE

Certified that this project report “ **INTRUSION HUNTER** ” is the bonafide work of

**SREEJHA.J [22AM050]**

**VISHNUPARGAVAN.V [22AM063]**

# KRISHNA PARESH RAICHURA [22AM021]

Who carried out the project work under my supervision

………………………………… …………………………………  **SIGNATURE SIGNATURE**

**Dr. R. SURESH M.sc., Ph.D Dr.S.SUMATHI M.E,Ph.D**

Professor & Head, **PROJECT GUIDE,**

Associate Professor,

Dept. of Science & Humanities(S & H),

Sri Eshwar College of Engineering, Dept. of Artificial Intelligence & Data

Coimbatore-641 202. Science,

Sri Eshwar College of

Engineering, Coimbatore-641202.

Submitted for the End Semester practical examination – Mini project work viva-voce held on ……………………

……………………… ………………………

**(Internal Examiner) (External Examiner)**

# DECLARATION

**SREEJHA.J [22AM050]**

**VISHNUPARGAVAN.V [22AM063]**

# KRISHNA PARESH RAICHURA [22AM021]

To declare that the project entitled “**INTRUSION HUNTER**”, submitted in partial fulfillment to University as the project work of Bachelor of Engineering (Computer Science and Engineering-AIML) Degree, is a record of original work done by us under the supervision and guidance of **Ms.Parvathy**, Assistant Professor, Department of Artificial Intelligence, Sri Eshwar College of Engineering, Coimbatore.

**Place:** Coimbatore

**Date:**

**[SREEJHA.J]**

**[VISHNUPARGAVAN.V]**

**[KRISHNA PARESH RAICHURA]**

Project guided by,

[Mr K.Parvathy]

## ACKNOWLEDGEMENT

The success of a work depends on a team and cooperation. We take this opportunity to express our gratitude and thanks to everyone who helped us in our project. We would like to thank the management for the constant support provided by them to complete this project.

It is indeed our great honour bounded duty to thank our **Chairman Mr. R. Mohanram**, for his academic interest shown towards the students.

We are indebted to our **Director Mr. R. Rajaram,** for motivating and providing us with all facilities.

We are indebted **to Dr. S. Sumathi, M.E., Ph.D. Head of Artificial Intelligence and Data Science** for having permitted us to carry out this project and giving the complete freedom to utilize the resources of the department.

We express our sincere thanks to our mini project Coordinator

**Dr.E.Saranya** Assistant Professor, Department of Computer Science and

Engineering for the valuable guidance and encouragement given, to us for this project.

We also extend our heartfelt thanks to our Project Guide

**Ms.K.Parvathy** Assistant Professor, Department of Artificial Intelligence and Data Science for providing us with her support and guidance which really helped us.

## TABEL OF CONTENTS

**1.INTRODUCTION…………………………………………………………………………..1**

Abstract

Future Scope

**2.BLOCK DIAGRAM………………………………………………………………………….9**

Overall Scenario Architecture

System Architecture

**3.IMPLEMENTATION………………………………………………………………………11**

System Implementation

Tools Used

**4.SCREENSHOTS……………………………………………………………………………..17**

Output

**4.CONCLUSION……………………………………………………………………………...20**

Conclusion

**5.REFERENCE…………………………………………………………………………………23**

**CHAPTER 1**

**INTRODUCTION**



## INTRODUCTION

In an increasingly interconnected world, where digital information flows are at the heart of every organization's operations, ensuring robust network security has become an imperative. With the ever-evolving landscape of cyber threats and malicious attacks, safeguarding sensitive data and protecting against unauthorized access have become paramount concerns. This project report delves into the realm of network security, with a primary focus on firewalls as a foundational defense mechanism, while also exploring their limitations and the need for supplementary security measures.

The purpose of this project is to comprehensively analyze firewalls' effectiveness as a crucial line of defense in protecting networks from external threats. Firewalls are instrumental in filtering and controlling network traffic, acting as a shield between trusted internal networks and the untrusted external environment, typically the internet. Through an in-depth examination of their functionalities, configurations, and various types, we aim to understand the role firewalls play in mitigating common cyber risks, such as Distributed Denial of Service (DDoS) attacks, malware infections, and unauthorized access attempts.

However, understanding the importance of acknowledging the limitations of firewalls is equally critical. While they excel in guarding against external threats, firewalls may not be as effective in thwarting attacks that originate from within the network or identifying existing malware on compromised systems. Furthermore, encrypted traffic poses a challenge for traditional firewall inspection, necessitating the exploration of alternative methods to ensure comprehensive network security.

The project report will explore real-world case studies and incidents to highlight instances where firewalls have proven effective and where they have encountered limitations. By drawing on established research, industry best practices, and expert insights, we aim to propose a defense-in-depth approach to network security. This approach entails integrating multiple security measures, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and endpoint protection, to fortify the network's security posture.

The ultimate goal of this project report is to equip readers with a holistic understanding of firewalls' role in network security, providing valuable insights into their deployment, configuration, and maintenance. Moreover, we aim to underscore the importance of a multi-layered security strategy and proactive cybersecurity practices to bolster an organization's ability to safeguard sensitive data, protect against evolving threats, and ensure uninterrupted business operations.

In the following sections, we will delve into the theoretical underpinnings of firewalls, analyze their strengths and weaknesses, and propose recommendations for a robust network security framework. Together, these insights will empower organizations to make informed decisions when designing and implementing their network security infrastructure, effectively safeguarding their digital assets in an ever-changing threat landscape.

## PROBLEM STATEMENT

In today's hyper-connected world, organizations face an ever-increasing array of cyber threats that can compromise sensitive data, disrupt operations, and tarnish reputations. As businesses heavily rely on interconnected networks to facilitate their daily operations and data exchange, ensuring robust network security has become a critical imperative. The problem at hand is to comprehensively analyze the existing network security infrastructure, with a primary focus on firewalls, and identify potential vulnerabilities and limitations that may expose the organization to cyber risks.

The project aims to address the following key issues

1. Firewall Effectiveness Assessment: Evaluate the effectiveness of existing firewalls in protecting the organization's network from external threats. Determine whether the current firewall configurations and rule sets adequately address common attack vectors, such as Distributed Denial of Service (DDoS) attacks, malware intrusions, and unauthorized access attempts.

2. Insider Threats and Malware Management: Examine the network's vulnerability to insider threats and investigate the measures in place to detect and mitigate such risks. Analyze the capability of the network's security infrastructure to identify and neutralize malware that may already be present within the network.

3. Encrypted Traffic Inspection: Investigate the challenges associated with inspecting encrypted traffic and assess the organization's capability to detect and prevent threats concealed within encrypted packets. Explore methods and technologies to enhance the inspection of encrypted data without compromising data privacy.

4. Limitations of Firewall Protection: Identify and critically analyze the limitations of firewalls as the primary defense mechanism. Investigate scenarios where firewalls may fail to provide adequate protection, such as advanced and zero-day attacks, and propose supplementary security measures to fill the gaps.

5. Defense-in-Depth Implementation: Design and propose a comprehensive defense-in-depth strategy that combines multiple security measures, including Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), network segmentation, endpoint protection, and user training. Assess how these layers of security can collectively reinforce the network's resilience against diverse cyber threats.

6. Industry Compliance and Best Practices: Analyze the organization's adherence to industry best practices, standards, and compliance regulations concerning network security. Evaluate whether the current security measures align with the latest guidelines and security frameworks.

By undertaking this project, we aim to provide valuable insights into the organization's network security infrastructure, identifying potential weaknesses and recommending practical solutions to fortify its defenses. The project's outcomes will enable the organization to make informed decisions in strengthening their cybersecurity posture, safeguarding critical data, and ensuring the continuous and secure flow of information throughout the network. Ultimately, the project aims to empower the organization to proactively address network security challenges and stay resilient against the ever-evolving landscape of cyber threats.

## FUTURE SCOPE

The project report paves the way for future developments in website security and network infrastructure. Potential areas for future exploration include the adoption of more advanced threat detection mechanisms, such as machine learning-based anomaly detection and behavior analysis, to enhance the network's ability to identify and respond to emerging and sophisticated threats. Security automation can streamline incident response procedures and optimize security tasks, reducing manual intervention and response time. Moreover, the report opens the possibility of expanding the organization's security measures to cloud environments, ensuring robust security configurations, data encryption, and access control for cloud-based resources.

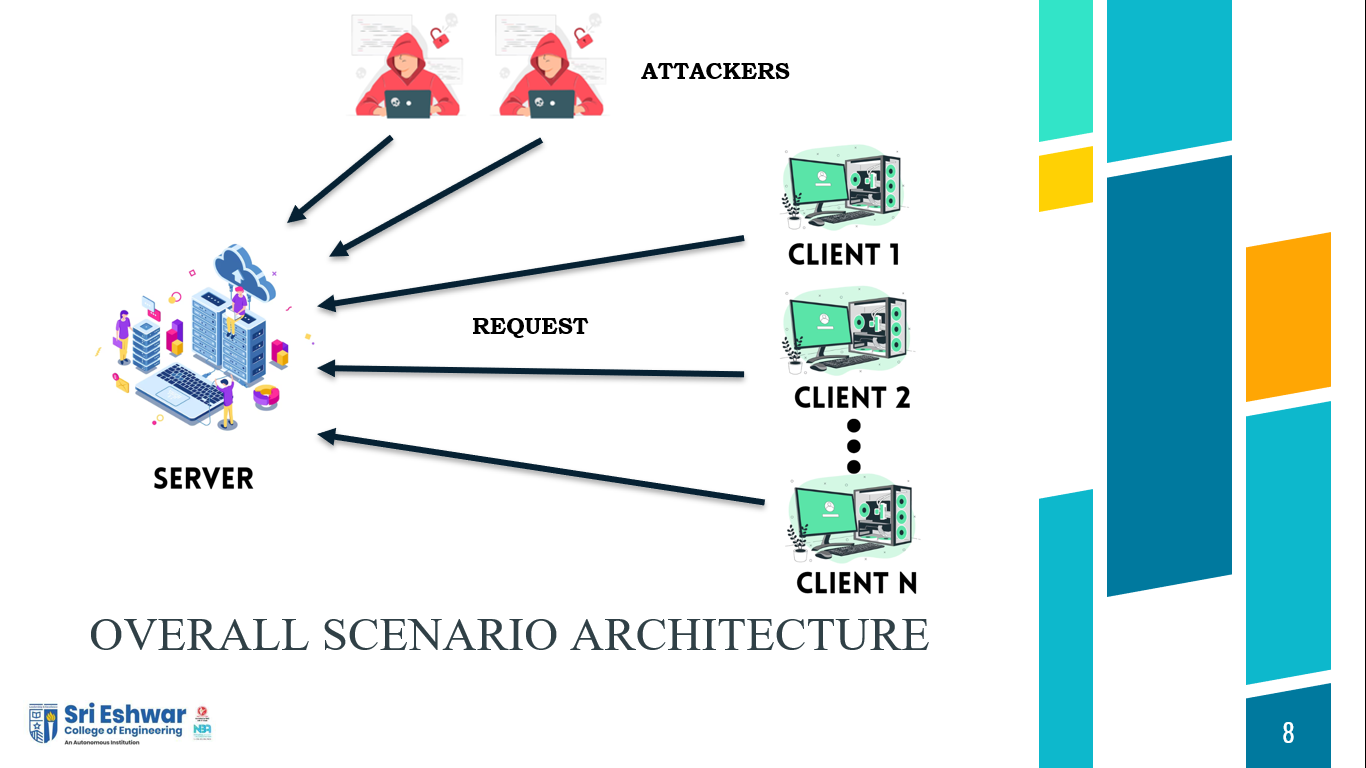
Additionally, incorporating multi-factor authentication (MFA) can add an extra layer of protection to user authentication, mitigating the risk of unauthorized access even if passwords are compromised. The implementation of a Security Information and Event Management (SIEM) system can provide a centralized view of security events and enable real-time threat analysis, facilitating a proactive response to potential security incidents. Regular security audits and red teaming exercises can help identify and address potential weaknesses in the network's defense, while integrating threat intelligence feeds can provide valuable insights into emerging threats and proactive defense strategies.

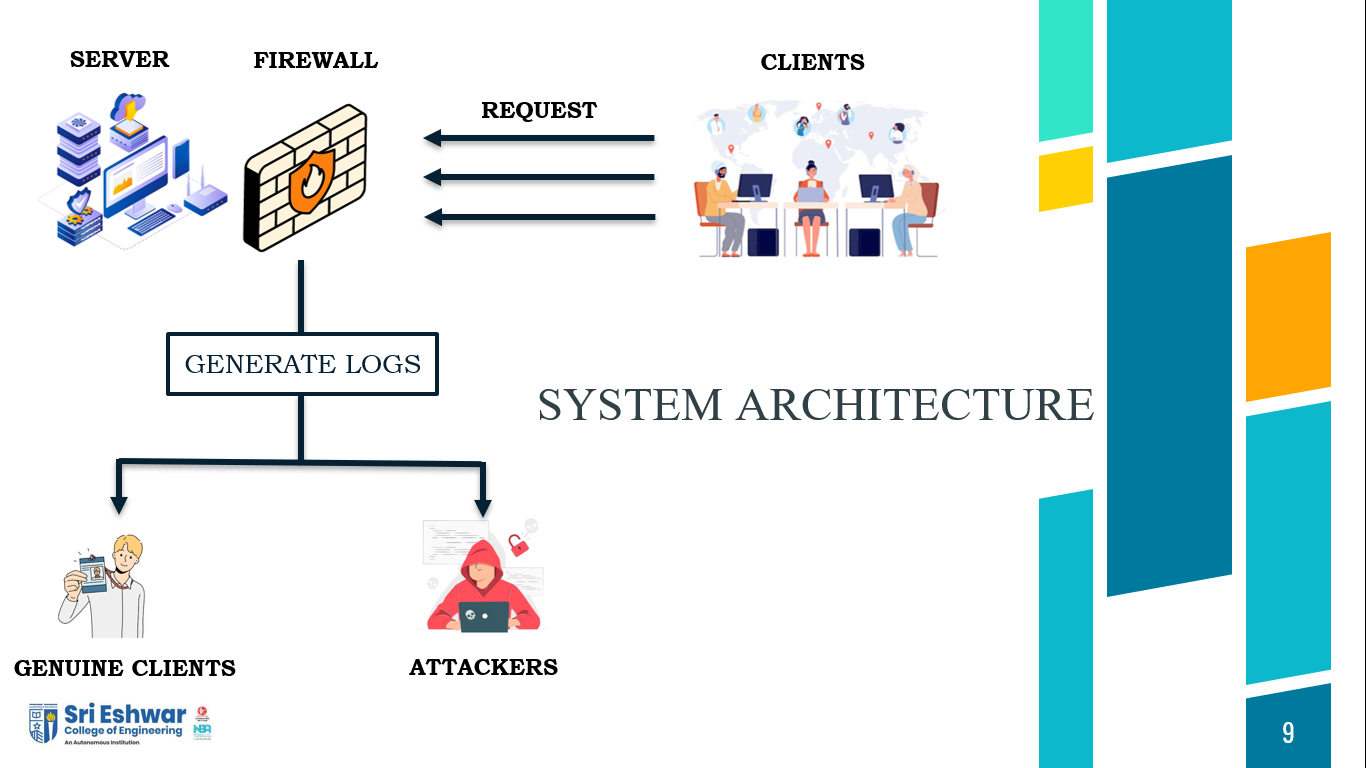
Furthermore, future work on data privacy enhancements can ensure compliance with data protection regulations like GDPR, safeguarding the privacy and security of users' sensitive information. Emphasizing these aspects in the future can significantly bolster the organization's cybersecurity posture, adapt to evolving cyber threats, and maintain a strong and secure online presence. By staying proactive and continuously improving security measures, the organization can effectively protect critical data and services from potential risks and ensure a resilient and secure digital environment for all stakeholders.

**CHAPTER 2**

**BLOCK DIGRAM**







**CHAPTER 3**

**IMPLEMENTATION**



## SYSTEM IMPLEMENTATION

**Introduction:**

In this implementation report, we detail the steps taken to enhance the security of our website using a combination of web development technologies (HTML, CSS, JS, SQL, PHP) and powerful security tools available in Kali Linux. The primary objective was to create a robust defense mechanism using firewall technologies (iptables), log monitoring (logcheck), and email server security (Postfix). This report outlines the key components of the implementation process, including setup, configuration, and results achieved.

**Website Development:**

We began the project by developing a dynamic and responsive website using HTML, CSS, JavaScript, SQL, and PHP. This website served as the foundation for the secure web application we aimed to protect with the firewall and Kali Linux tools.

**Firewall Configuration using iptables:**

To protect our website from external threats and unauthorized access attempts, we implemented iptables, a powerful firewall tool in Kali Linux. The firewall was configured to allow only necessary ports for web traffic (e.g., HTTP on port 80 and HTTPS on port 443) while blocking all other incoming and outgoing traffic by default.

**Log Monitoring with logcheck:**

Log monitoring is a crucial aspect of identifying potential security incidents. We integrated logcheck into our system to monitor system logs and identify suspicious activities, potential attacks, or unauthorized access attempts. Logcheck was configured to generate alerts for critical log entries, enabling timely response to security events.

**Email Server Security with Postfix:**

Securing the email server was another key aspect of our website's overall security. We utilized Postfix, a widely-used mail transfer agent, to ensure secure email communication. The email server was configured to prevent unauthorized access and protect against email-based attacks.

**Web Application Firewall (WAF) Integration:**

To add an extra layer of security to our website, we incorporated a Web Application Firewall (WAF) as a reverse proxy. The WAF was configured to inspect and filter incoming web traffic, mitigating common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), and other malicious attacks.

**Penetration Testing and Vulnerability Assessment:**

To ensure the effectiveness of our security measures, we conducted penetration testing and vulnerability assessments using various tools available in Kali Linux. This step allowed us to identify and remediate any potential security weaknesses in the website and server configurations.

**Monitoring and Incident Response:**

We established a monitoring system to continuously track and analyze network traffic, firewall logs, and server activities. In the event of a security incident, predefined incident response procedures were put into action to minimize the impact and prevent further escalation.

**Results and Conclusion:**

The implementation of Kali Linux tools, firewall technologies, and security measures significantly improved the overall security posture of our website. The combination of iptables, logcheck, and Postfix provided an effective defense against external threats, unauthorized access, and potential attacks. Additionally, the integration of a WAF enhanced protection against web application vulnerabilities.

**Future Recommendations:**

While the implemented security measures demonstrated their effectiveness, continuous improvement is essential in the face of evolving threats. We recommend regular updates to security configurations, conducting periodic vulnerability assessments, and staying up-to-date with the latest security patches for all components.

In conclusion, the successful implementation of the firewall and Kali Linux tools resulted in a fortified website with enhanced protection against cyber threats. By combining robust web development practices with advanced security measures, we achieved a secure and reliable online presence. The knowledge gained from this implementation will serve as a valuable resource in creating and maintaining secure web applications in the future.

**TOOLS USED**

**HTML, CSS, JS, SQL, PHP:** These are fundamental web development technologies used to create the website. HTML provides the structure of the web pages, CSS styles the presentation, JavaScript adds interactivity and dynamic elements, SQL handles the database operations, and PHP is used for server-side scripting to process user requests and generate dynamic content.

**Kali Linux:** Kali Linux is a popular Linux distribution specially designed for penetration testing, digital forensics, and cybersecurity tasks. It includes a wide range of security tools that aid in testing and securing systems against various vulnerabilities and threats.

**iptables:** iptables is a powerful firewall tool in Linux that allows administrators to configure packet filtering rules for incoming and outgoing network traffic. It is a crucial component for securing the website by controlling access to specific ports and IP addresses.

**logcheck:** logcheck is a log monitoring tool used to analyze system logs and generate alerts for critical log entries. It helps in detecting potential security incidents and unauthorized access attempts by monitoring log files and identifying suspicious activities.

**Postfix:** Postfix is a popular mail transfer agent (MTA) used to manage and route email messages. It plays a critical role in securing the organization's email communication by preventing unauthorized access and protecting against email-based attacks.

**Web Application Firewall (WAF):** A WAF is a security tool that acts as a reverse proxy, inspecting and filtering web traffic before it reaches the web server. It helps protect web applications from various attacks, such as SQL injection, cross-site scripting (XSS), and other common web vulnerabilities.

**Penetration Testing Tools:** Kali Linux includes a variety of penetration testing tools, such as Nmap, Nikto, Burp Suite, and Metasploit. These tools are used to simulate real-world attacks and vulnerabilities, helping identify weaknesses in the network and web application.

**Vulnerability Assessment Tools:** Kali Linux also provides tools like OpenVAS and Nexpose for conducting vulnerability assessments. These tools scan the network and web application for known vulnerabilities, providing a comprehensive report of potential weaknesses.

**Monitoring Tools:** Monitoring tools are used to track network traffic, system activities, and firewall logs in real-time. They enable proactive detection of security incidents and suspicious behavior, allowing for timely response and mitigation.

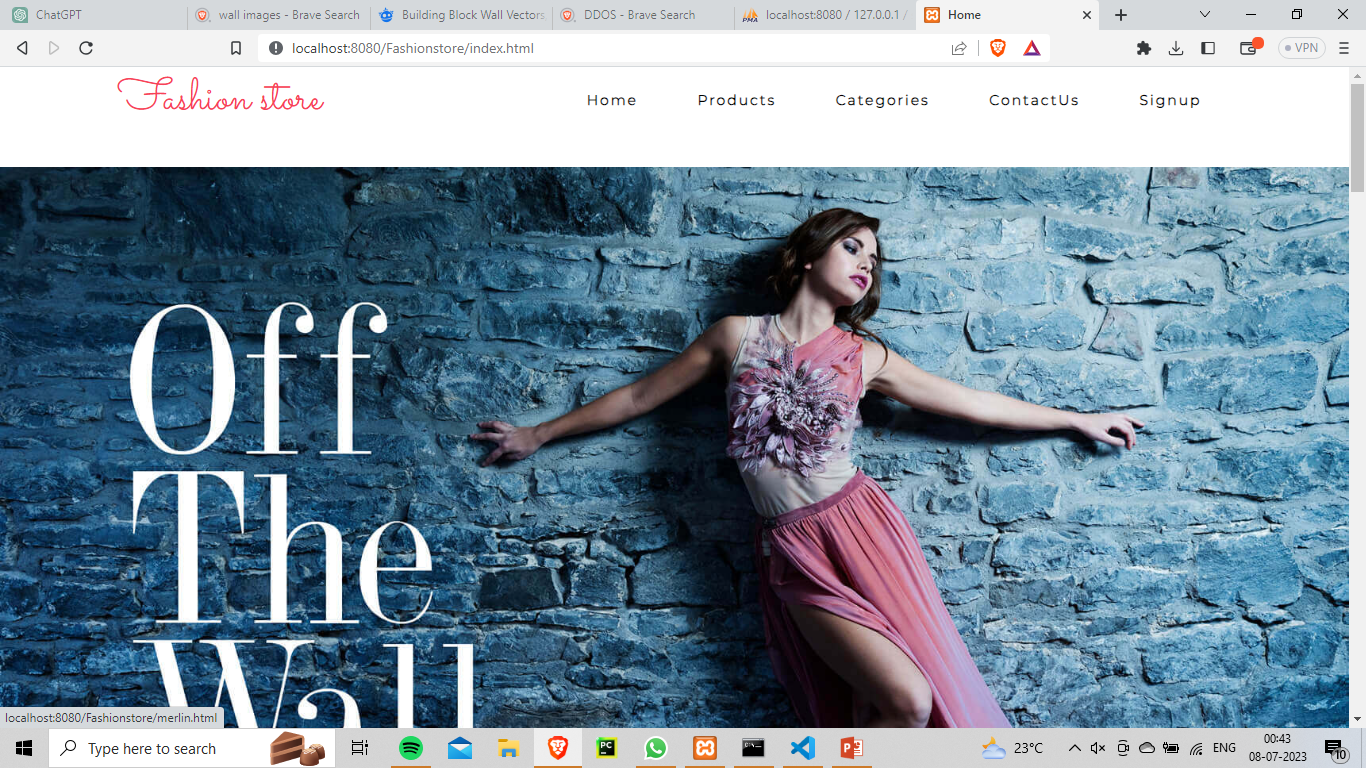
**Incident Response Procedures:** Incident response procedures are predefined plans and protocols that guide the organization's response to security incidents. These procedures outline the steps to be taken in the event of a breach or cyber attack to minimize the impact and prevent further damage.

**` CHAPTER 4**

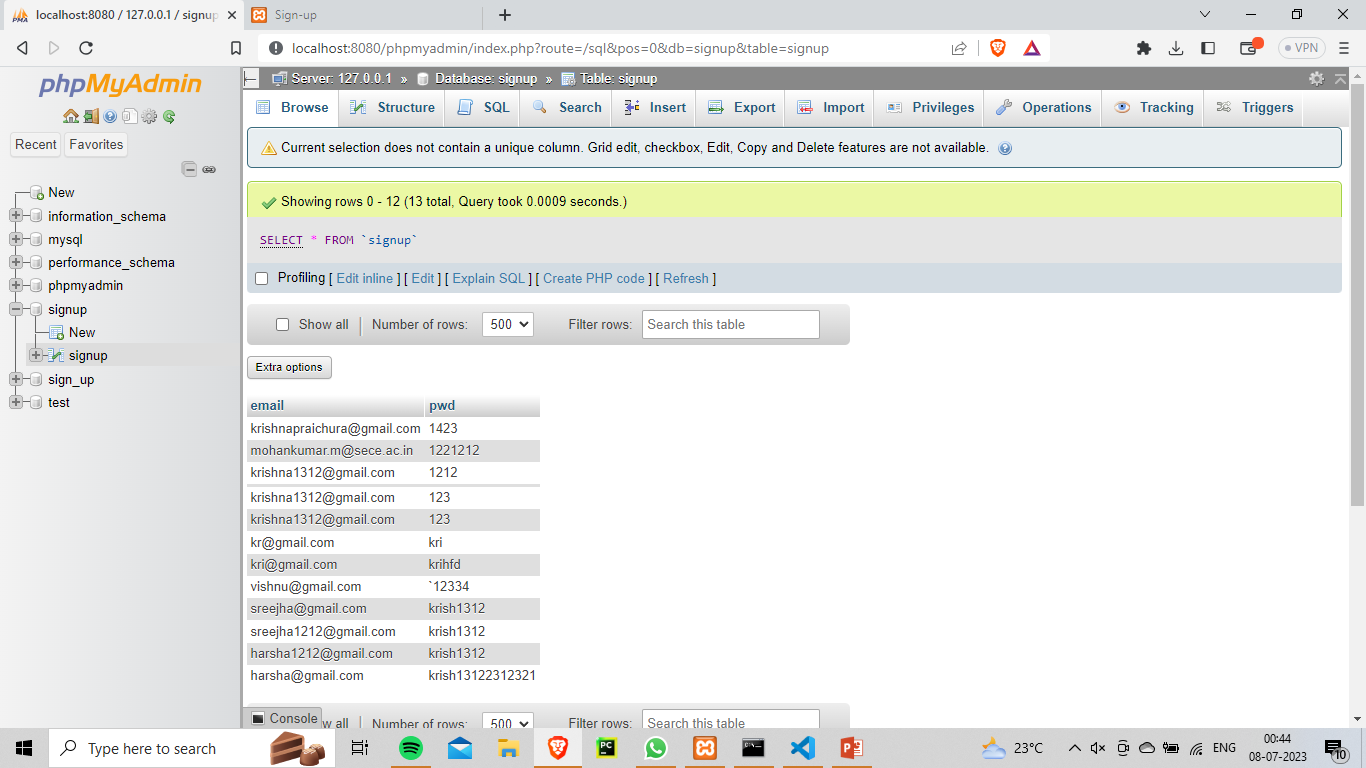
**OUTPUT**

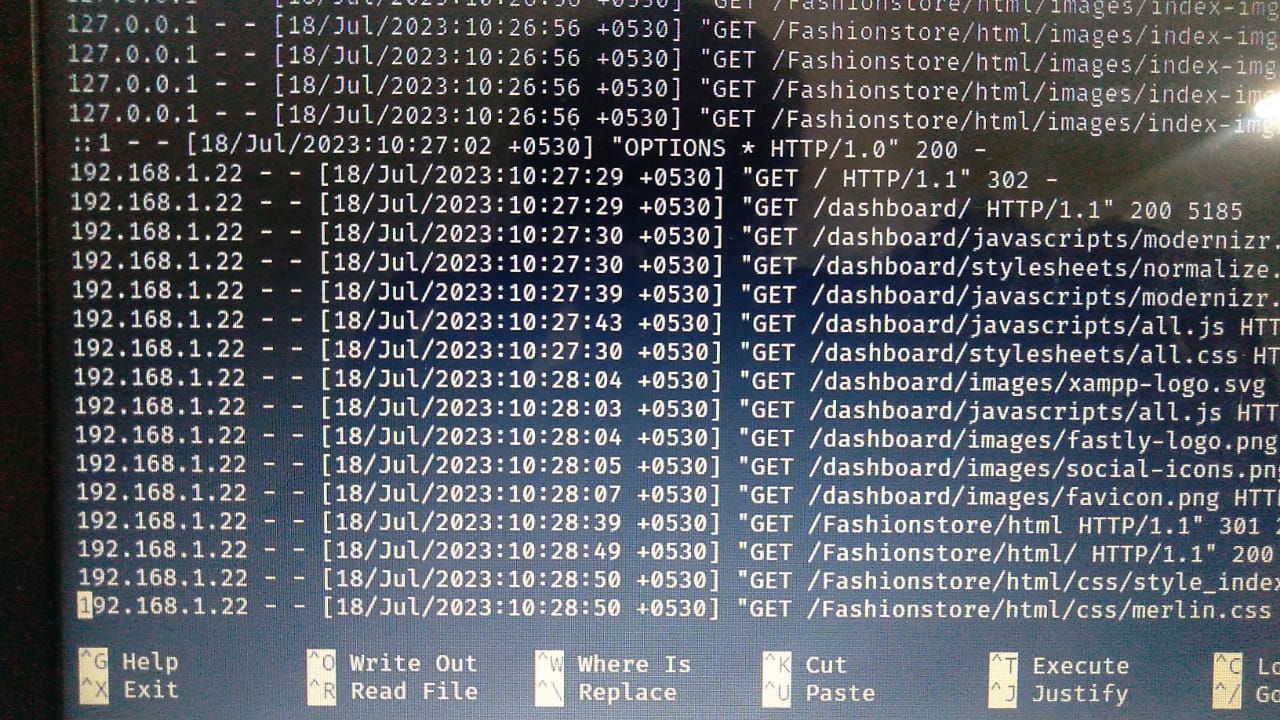


**Fig 1.1** The below screenshot is the website we hosted and created a server

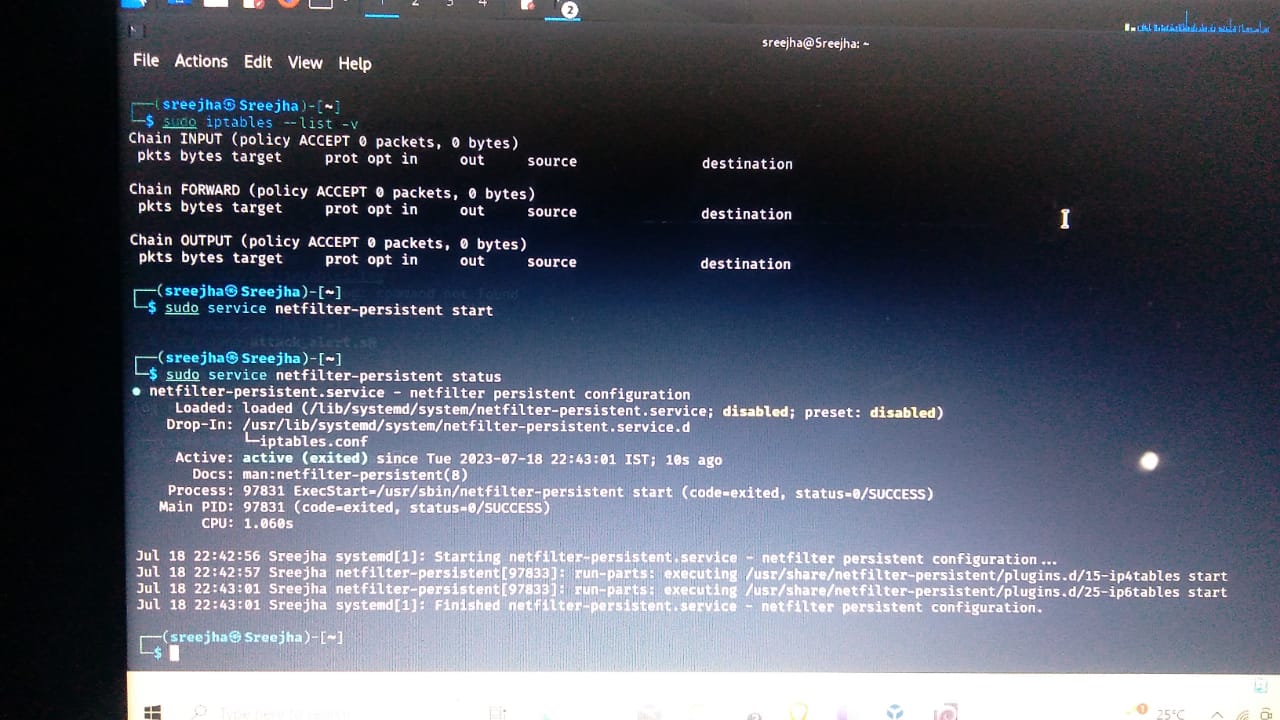


**Fig 1.2** The below screenshot is the database of the website

****



**Fig 1.3** The below screenshot is the mail generation



**Fig 1.4** The below screenshot is enabling the firewa

**CHAPTER 5**

**CONCLUSION**



## CONCLUSION

In conclusion, the implementation of security measures using a combination of web development technologies and Kali Linux tools has significantly strengthened the security of the website and network infrastructure. Through the integration of HTML, CSS, JS, SQL, and PHP, we developed a dynamic and responsive website, serving as the foundation for a secure web application.

By leveraging Kali Linux tools, such as iptables, logcheck, Postfix, and a Web Application Firewall (WAF), we successfully established a robust defense mechanism against external threats and potential cyber attacks. The iptables firewall configuration allowed precise control of network traffic, while logcheck enabled real-time log monitoring, providing timely alerts for critical log entries.

In addition to securing the network, we prioritized email server security using Postfix to safeguard email communications from potential attacks. Furthermore, the WAF integration acted as an extra layer of protection, mitigating web application vulnerabilities effectively.

Throughout the implementation, we conducted thorough penetration testing and vulnerability assessments using Kali Linux tools, identifying and addressing potential security weaknesses proactively. Moreover, we established a monitoring system for continuous network traffic analysis and implemented predefined incident response procedures for prompt action in case of security incidents.

One notable enhancement is the addition of an automated email generation and notification system. Whenever a critical security event is detected, such as a potential breach attempt or suspicious activity, an email alert is automatically generated and sent to the administrator's designated address. This proactive measure enables immediate response to security incidents, minimizing their impact and facilitating swift remediation.

In conclusion, the successful implementation of these security measures showcases the synergy between web development practices and cybersecurity technologies. By embracing this holistic approach, we have fortified our website, ensuring the protection of sensitive data, thwarting potential threats, and providing uninterrupted services. As the cyber landscape continues to evolve, adherence to industry best practices and continuous vigilance will be crucial in maintaining a secure and resilient online presence.

**CHAPTER 6**

**REFERENCE**



## [1.Configuration of Microsoft ISA Proxy Server and Linux Squid Proxy Server – book\](https://www.amazon.com/dp/1723956074?tag=uuid10-20" \t "_blank)

2. [SonicWall Firewall Administrator Journal, Certification Exam Preparation Notebook, examination study writing notebook, Office writing notebook](https://www.amazon.com/dp/B091DWWB8D?tag=uuid10-20" \t "_blank)

3. <https://www.kali.org/> - KALI LINUX USAGE

4. <https://community.checkpoint.com/t5/Policy-Management/Finding-Log-by-the-UserCheck-Reference-Number/td-p/12596>

5.https://www.google.com/search?tbm=vid&q=LOGCHECK%20REFERENCE#fpstate=ive&vld=cid:f1d5d138,vid:JAGNcrP3qFI

6.Cyber Security : Issues and Current Trends- Nitul Data