Industry Project

Report

On

WAF and Network Firewall

Developed By: -

Prajapati Sahil Kantibhai (2062172006)

Urmik Pandya (21162172006)

Guided By:-

Prof. Aniket Patel (Internal Guide)

Mr. Jay Kotadiya (Cyber Security Analyst)

Submitted to

Faculty of Engineering and Technology

Institute of Computer Technology

Ganpat University

Year – 2024

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Institute of Computer Technology

CERTIFICATE

This is to certify that the **Industry** Project work entitled **"Creating WAF & Network Firewall"** by Prajapati Sahil Kantibhai (Enrollment No.20162171022) and Urmik Pandya (21162172006) of Ganpat University, towards the partial fulfillment of requirements of the degree of Bachelor of Technology – Computer Science and Engineering, carried out by them in the CSE (CS) Department at IBhavan. The results contained in this Project have not been submitted in part or full to any other University / Institute for award of any other Degree/Diploma.

Name & Signature of Internal Guide

Name & Signature of Head

Place: ICT - GUNI

Date:

ACKNOWLEDGEMENT

Industry Internship project is a golden opportunity for learning and self-development. I consider myself very lucky and honored to have so many wonderful people lead me through in completion of this project. First and foremost, I would like to thank Dr. Rohit Patel Principal, ICT, and Prof. Dharmesh Darji, Head, ICT who gave us an opportunity to undertake this project. My grateful thanks to Prof. Aniket Patel and Mr. Jay Kotadiya (Internal & External Guides) for their guidance in project work Creating WAF & Network Firewall, who despite being extraordinarily busy with academics, took time out to hear, guide and keep us on the correct path. We do not know where would have been without his/her help. CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Prajapati Sahil Kantibhai (Enrollment No:20162171022)

ABSTRACT

This paper introduces a firewall designed to bolster network security. By implementing advanced packet inspection techniques, the firewall intelligently monitors and controls traffic based on active connections, bolstered by features like access control lists, network address translation, and intrusion detection mechanisms. Leveraging modular architecture and open- source technologies like Python and C, the firewall ensures both flexibility and efficiency. Through comprehensive testing in simulated environments, its effectiveness in mitigating various threats is evaluated, affirming its role as a robust solution for modern cyber security challenges. Future directions include refinement and real-world deployment to validate its efficacy further.

INDEX

CHAPTER: 1 INTRODUCTION

CHAPTER 1 INTRODUCTION

In today's interconnected world, network security is of paramount importance to safeguard sensitive data, systems, and infrastructure from unauthorized access, malicious activities, and cyber threats. Among the plethora of security measures available, network-based firewalls stand as one of the foundational elements in protecting networks from external threats.

A network-based firewall acts as a barrier between an internal network and external networks, such as the internet. It serves as a gatekeeper, monitoring and controlling incoming and outgoing traffic based on predetermined security rules and policies. By inspecting packets of data as they traverse the network, network-based firewalls can enforce access control and mitigate potential risks by blocking or allowing traffic according to predefined criteria.

A Web Application Firewall (WAF) is a security solution designed to protect web applications from various online threats and attacks. It acts as a barrier between the web application and the internet, monitoring and filtering HTTP traffic between the two. WAFs analyze incoming traffic to detect and block malicious requests, such as SQL injection, cross-site scripting (XSS), and other common web vulnerabilities. By inspecting and filtering web requests based on predefined rules and policies, WAFs help prevent unauthorized access, data breaches, and other cyber threats, thus enhancing the overall security posture of web applications.

CHAPTER: 2 PROJECT SCOPE

CHAPTER 2 PROJECT SCOPE

The project scope encompasses the design, implementation, and deployment of a robust network-based firewall solution aimed at bolstering the organization's network security posture. The primary objectives revolve around establishing a secure perimeter between the internal network and external networks, such as the internet, while enforcing stringent access control and threat prevention measures. This includes configuring the firewall with advanced features like stateful inspection, application layer filtering, and intrusion detection, as well as integrating VPN support for secure remote access. Additionally, the scope entails setting up logging and reporting mechanisms to monitor network activity, track security events, and ensure compliance with industry regulations. The project will involve collaboration among key stakeholders, including the IT security team and network administrators, to ensure successful implementation within the defined timeline and budget. Constraints such as adherence to organizational policies and regulatory requirements, along with risk management considerations, will be carefully addressed throughout the project lifecycle to mitigate potential disruptions and ensure the effectiveness of the firewall solution.

The project scope for implementing a Web Application Firewall (WAF) includes deploying a security solution to protect web applications from various online threats. This involves configuring the WAF to monitor and filter incoming web traffic, detecting and blocking malicious requests like SQL injection and cross-site scripting. Regular monitoring and maintenance ensure ongoing effectiveness against evolving threats, enhancing the overall security of web applications.

CHAPTER: 3 SOFTWARE AND HARDWARE REQUIREMENTS

CHAPTER 3 SOFTWARE AND HARDWARE REQUIREMENTS

Minimum Hardware Requirements

1. CPU: Dual-core (1.5 GHz or higher).
2. RAM: 2 GB minimum.
3. Storage: 20 GB disk space.
4. Network Interface: Gigabit Ethernet.
5. Form Factor: Rack-mountable server or virtual machine.

Minimum Software Requirements

1. OS: Linux (e.g., Centos, Ubuntu) or Windows Server.
2. Dependencies: Required libraries specified by vendor.
3. Firewall Software: Vendor-provided package.
4. Management: Tools for configuration and monitoring.

CHAPTER: 4 PROCESS MODEL

Network Firewall :

- **Packet Filtering** : Network firewalls inspect packets at the network layer (typically TCP/IP layers 3 and 4) based on predefined rules, allowing or blocking traffic based on source and destination IP addresses, ports, and protocols.
- **Stateful Inspection:** Network firewalls maintain state information about active connections to Distinguish between legitimate and unauthorized traffic, enhancing security.
- **Application Layer Filtering (Proxy Firewall)**: Advanced network firewalls can inspect traffic at The application layer (Layer 7) to provide additional security by analyzing application-specific Protocols and content.
- **Virtual Private Network (VPN) Support:** Some network firewalls offer VPN capabilities to Secure communications between remote users or branch offices and the corporate network.
- **Logging and Reporting:** Network firewalls log network traffic events, such as allowed connections, blocked traffic, and intrusion attempts, providing visibility into network activity and Security events.
- **Regular Updates and Maintenance:** Network firewalls require regular updates to maintain effectiveness against emerging threats and vulnerabilities, including updating firmware, signature databases, and rule sets.

Web Application Firewall (WAF) :

- **Detection and Analysis:** Incoming HTTP/HTTPS traffic is analyzed in real-time to identify potential threats and vulnerabilities within web applications.
- **Rule Evaluation:** WAF applies predefined rules and policies specific to web application security, Such as signature-based detection, behavior analysis, and anomaly detection.
- **Request Blocking:** Malicious requests are blocked based on rule evaluations, preventing attacks Like SQL injection, cross-site scripting (XSS), and other web-based threats from reaching the application.
- **Logging and Reporting:** WAF logs all traffic and security events for analysis and generates reports to provide insights into detected threats and system performance.
- **Continuous Monitoring and Updating:** Regular updates to rules and policies ensure that the WAF Remains effective against evolving threats.

CHAPTER: 5 PROJECT PLAN

CHAPTER 5 PROJECT PLAN

5.1 List of Major Activities

Task: -1 Research work and Requirements Gathering
Task: -2 Define Modules of the project
Task: -3 Packet Capturing and Tracing
Task: -4 Discover Live Hosts on the network
Task: -5 Rules Defined for Packets Captured
Task: - 6 Capturing and Detecting Malicious Packet
Task: -7 Blocking and Unblocking TCP and UDP rules
Task: -8 Started work on WAF made Flask webpage
Task: - 9 Filtration of SQL injection payloads onwebpage
Task:-10 Filtration of XSS payloads on web page
Task:-11 Filter Malicious request sent in different method
Task:-12 Filtration of OS Command injection on webpage
Task:-13 Filtration of RFI\LFI attack on web page
Task:-14 Filtration of Path Traversal payloads on webpage
Task:-15 Filtration of Linux based commands payloads
Task:-16 Created UI\UX design of our Web page
Task:-17 Blocking any malicious payload and Sending mail
Task:-18 Added SSL certificate to our web page

5.2 Estimated Time Duration in Days

#	NAME	ASSIGNEE	STATUS	DUE DATE	PRIORITY
1	Research work and Requireme...		COMPLETE	1/12/24	
2	Define Modules of the project		COMPLETE	1/18/24	
3	Packet Capturing and Tracing ...		COMPLETE	1/26/24	
4	Discover Live Hosts on the net...		COMPLETE	5 days ago	
5	Define Dataset of Inbound and...		IN PROGRESS	4/9/24	

+ New Task

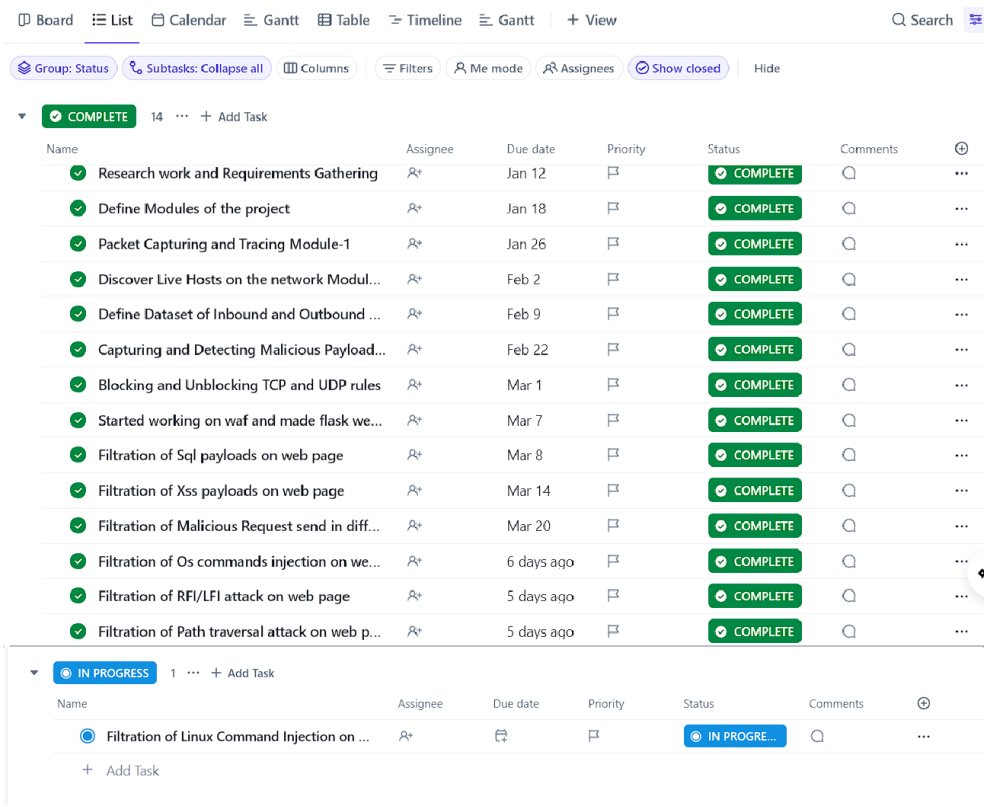


Fig 5.2 Task Completion Estimated Time Duration in Days

CHAPTER: 6 IMPLEMENTATION DETAILS

6.1 Research work and Requirements Gathering

Network Security Fundamentals:

Review fundamental concepts of network security, including encryption, authentication, authorization, and auditing (AAA).
Understand common attack vectors, such as malware, phishing, denial-of-service (DOS), and man-in-the-middle (MITM) attacks.

Firewall Technologies:

Explore different types of firewalls, including stateful, stateless, application-layer, and next-generation firewalls (NGFW).
Understand how stateful firewalls operate by maintaining connection state and enforcing rules based on the state of network traffic.

Packet Filtering and Inspection:

Study packet filtering techniques used in firewalls to inspect and control traffic based on defined criteria, such as IP addresses, port numbers, and protocol types.
Learn about deep packet inspection (DPI) methods for analyzing packet contents at the application layer to detect and block suspicious or malicious traffic.

Access Control and Security Policies:

Investigate the principles of access control and security policies governing firewall configurations.
Explore methods for defining and enforcing firewall rules, including allow/deny lists, port-based filtering, and application-aware filtering.

Network Address Translation (NAT):

Research NAT techniques used in firewalls to translate private IP addresses to public IP addresses and vice versa, enabling connectivity between different network segments.
Understand the various types of NAT, such as static NAT, dynamic NAT, and port address translation (PAT).

Intrusion Detection and Prevention:

Learn about intrusion detection and prevention systems (IDPS) integrated with firewalls to detect and mitigate potential security threats.
Explore signature-based and anomaly-based detection methods for identifying known and unknown attacks.

Security Standards and Compliance:

Familiarize yourself with industry standards and regulatory requirements related to network security and firewall implementations.
Research compliance frameworks such as PCI DSS, HIPAA, GDPR, and ISO/IEC 27001 to ensure alignment with legal and regulatory obligations.

Emerging Technologies and Trends:

Stay updated on emerging technologies and trends in firewall design and network security, such as cloud-based firewalls, Software-Defined Networking (SDN), and threat intelligence integration.
Explore advancements in artificial intelligence (AI) and machine learning (ML) for enhancing firewall capabilities, such as automated threat detection and adaptive security policies.

Vendor Solutions and Open-Source Tools:

Evaluate commercial firewall solutions offered by vendors and compare features, performance, and pricing.
Explore open-source firewall software like iptables, nftables, and pfSense for building custom firewall solutions tailored to specific requirements.

Case Studies and Best Practices:

Analyze real-world case studies and best practices for implementing stateful firewalls in different environments, industries, and use cases.

Learn from successful firewall deployments and security incidents to identify lessons learned and avoid common pitfalls.

6.2 Define Modules of this Project

Packet Inspection Module:
Responsible for analyzing incoming and outgoing network packets.
Implements stateful packet inspection to track the state of network connections.
Determines whether packets should be allowed, denied, or flagged for further analysis.

Rule Engine Module:
Manages the firewall rules and policies.
Evaluates incoming packets against the defined rules to make filtering decisions.
Supports the creation, modification, and deletion of firewall rules based on user-defined criteria.

Connection Tracking Module:
Maintains a state table to track the state of network connections.
Records information about established connections, including source and destination IP addresses, ports, and protocol types.
Enables the firewall to enforce stateful inspection by referencing the connection state during packet processing.

Access Control Module:
Enforces access control policies to regulate network traffic.
Implements access control lists (ACLs) to permit or deny specific types of traffic based on source and destination addresses, ports, and protocols.
Supports the creation and management of ACL rules for different network segments or user groups.

Network Address Translation (NAT) Module:
Handles network address translation (NAT) functions, such as port forwarding, dynamic NAT, and static NAT.
Translates private IP addresses to public IP addresses and vice versa to enable communication between internal and external networks.
Manages NAT mappings and maintains translation tables for tracking address translations.

Logging and Reporting Module:
Logs firewall events, including allowed connections, denied packets, and security rule violations.
Provides reporting capabilities to generate summaries and statistics on network traffic, security incidents, and firewall performance.
Supports integration with external logging and reporting systems for centralized monitoring and analysis.

Configuration Management Module:
Handles the configuration of firewall settings and parameters.
Allows administrators to define and customize firewall policies, rules, and preferences.
Provides an interface for managing firewall configurations through command-line tools, graphical user interfaces (GUIs), or configuration files.

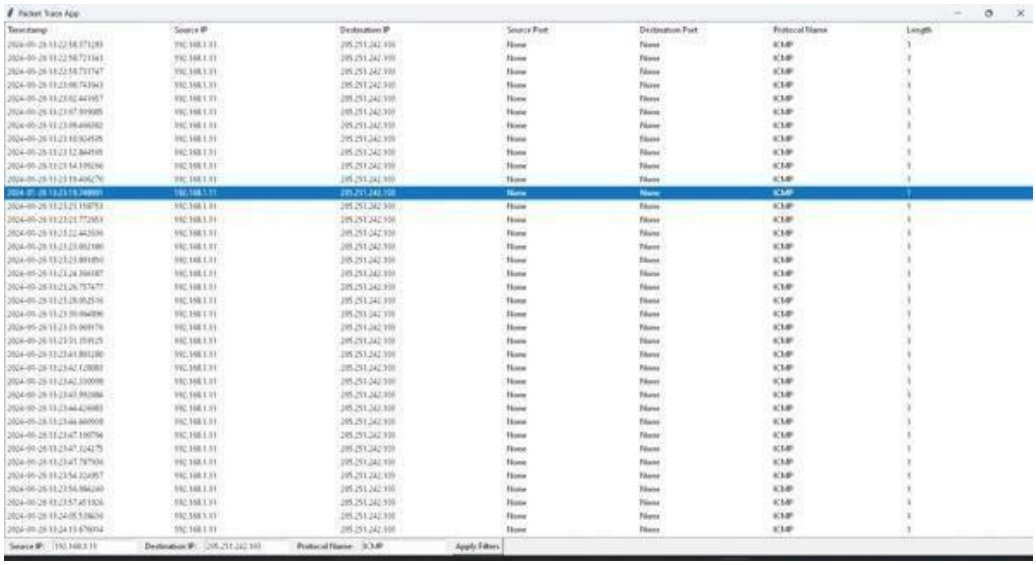
Intrusion Detection/Prevention Module:
Integrates intrusion detection and prevention capabilities into the firewall.
Monitors network traffic for signs of suspicious or malicious activity using signature-based and anomaly-based detection techniques.
Takes proactive measures to block or mitigate potential security threats identified by the intrusion detection system.

User Interface Module:
Provides a user-friendly interface for interacting with the firewall system.
Includes command-line interfaces (CLIs), web-based management consoles, or APIs for programmatic access.
Allows administrators to configure firewall settings, monitor network activity, and view security alerts and logs.

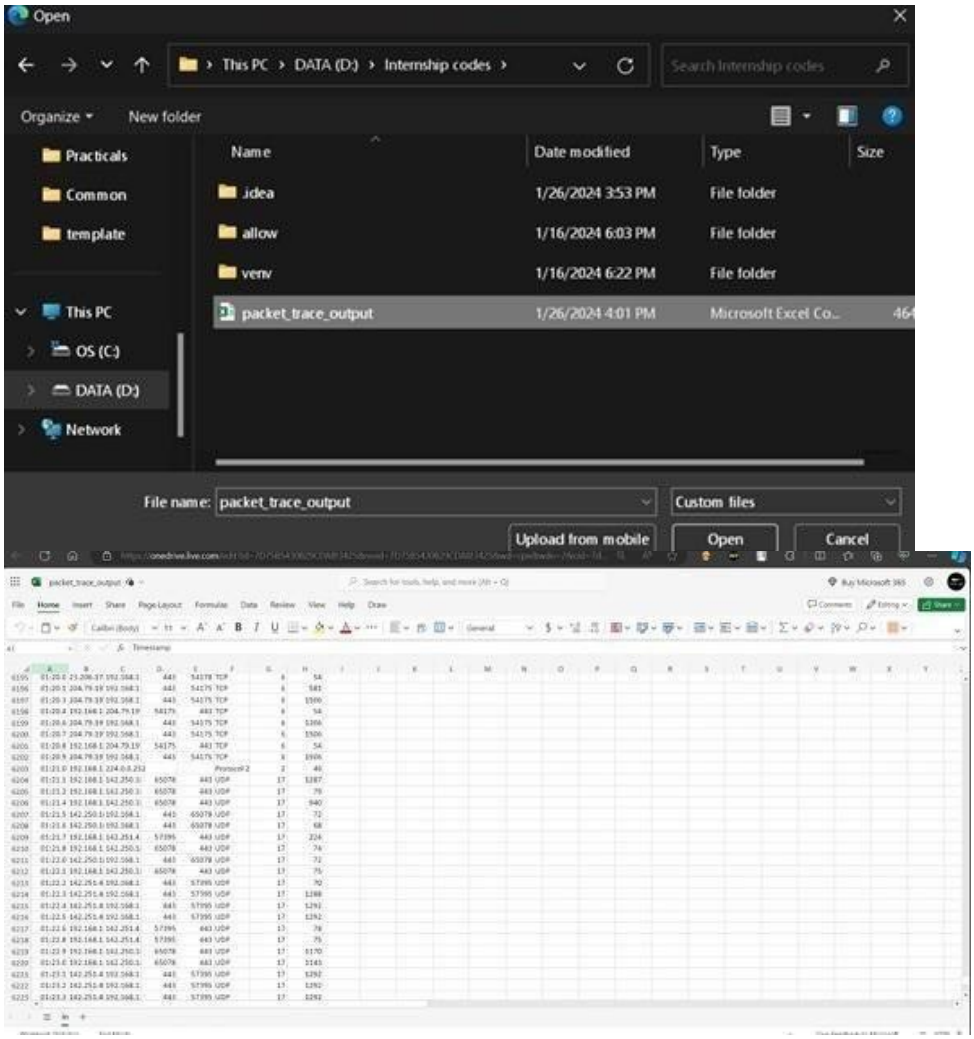
Performance Optimization Module:
Optimizes firewall performance and resource utilization to ensure efficient packet processing.
Implements techniques such as connection caching, packet queuing, and hardware acceleration to improve throughput and reduce latency.
Monitors system resources and adjusts firewall configurations dynamically to maintain optimal performance under varying load conditions.

6.3 Packet Tracking and Capturing

Packet tracing code this code trace all the traffic of network and captures the details like source IP, destination IP, source port, destination port, Port number and length of packets. Running the packet tracer code which captures the packets transferring on the network from source to destination with information like source and Destination IP's, source and destination ports, protocol name, packets length and with date and time Scanning has started .Now check different protocols are being captured or not. Checking ICMP Protocol to check it you should ping any website.



Your collected data is also stored in .CSV format file.



6.4 Discover Live Host on the Network

Performs network scanning to identify live hosts within the network or specified IP ranges.

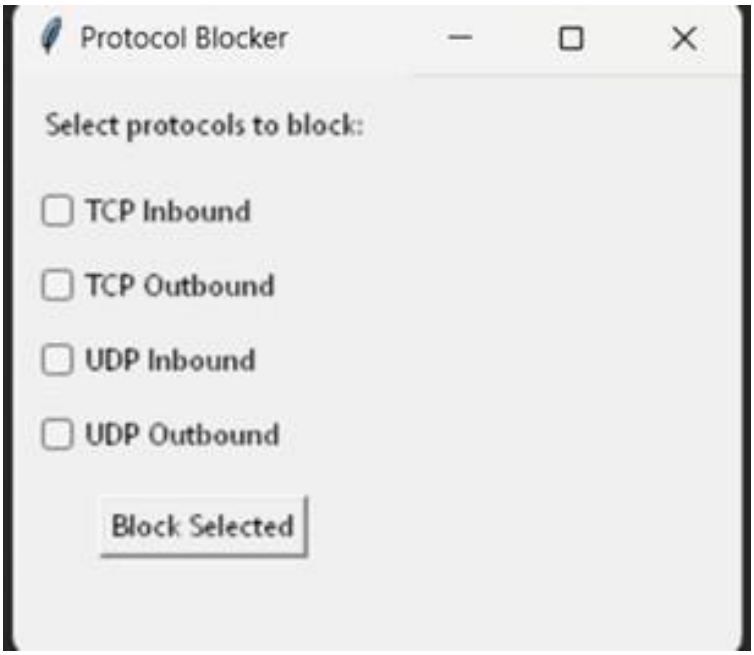
Utilizes techniques such as ICMP ping sweeps, ARP scanning, or TCP SYN scans to probe for active hosts. Collects information about discovered hosts, including IP address, Mac address, and hostnames and OS information.

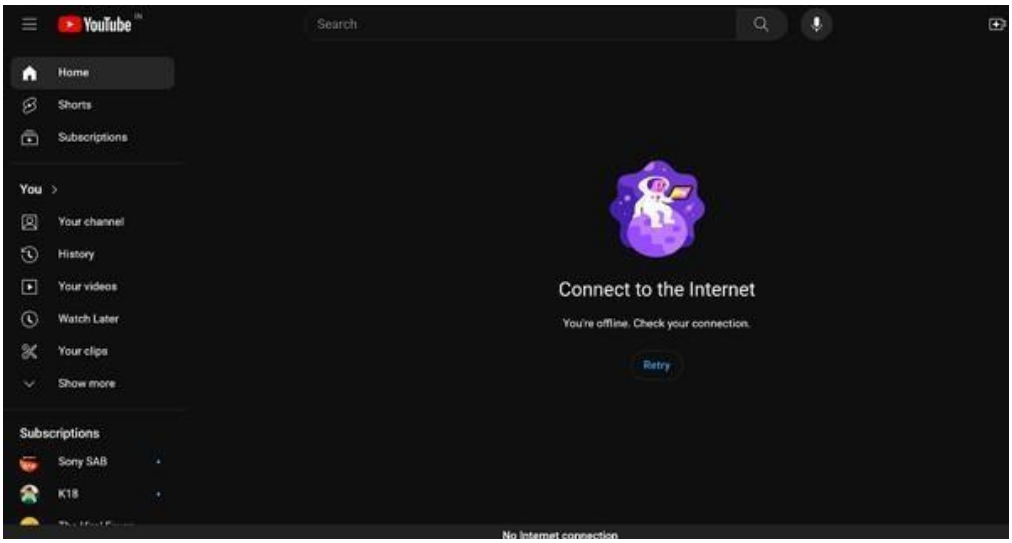
6.5 Capturing and Detecting Malicious Packet

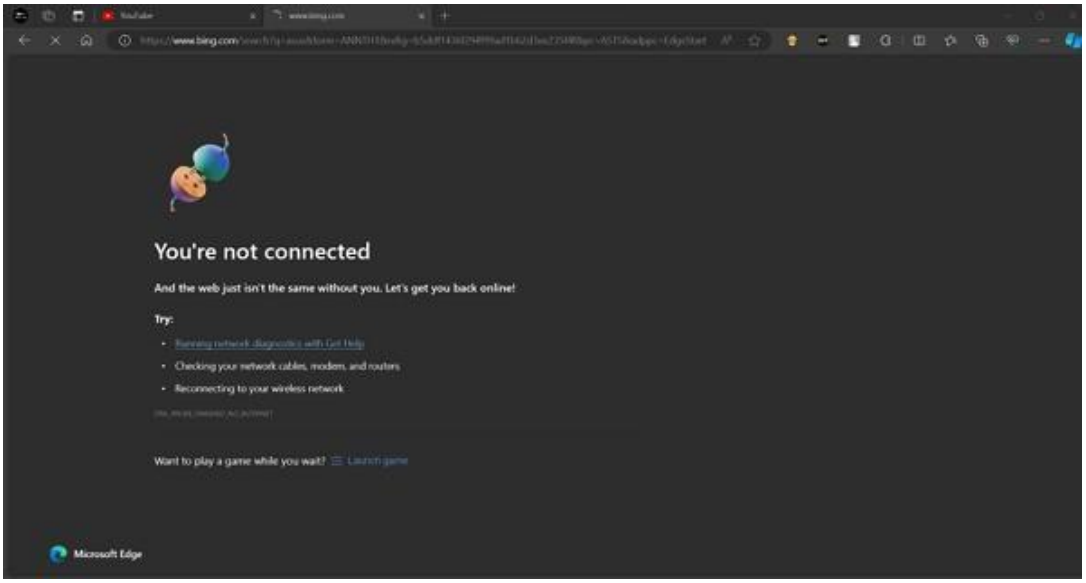
Sending Malicious Packet on mentioned IP in script this packet contains “malware123” string which is pattern for detection in detection script it will capture this packet and check if the packet contains any string like “malware123” if yes than it will show a message “This packet contains malware” and show the packet details like source IP, destination IP, and raw data.

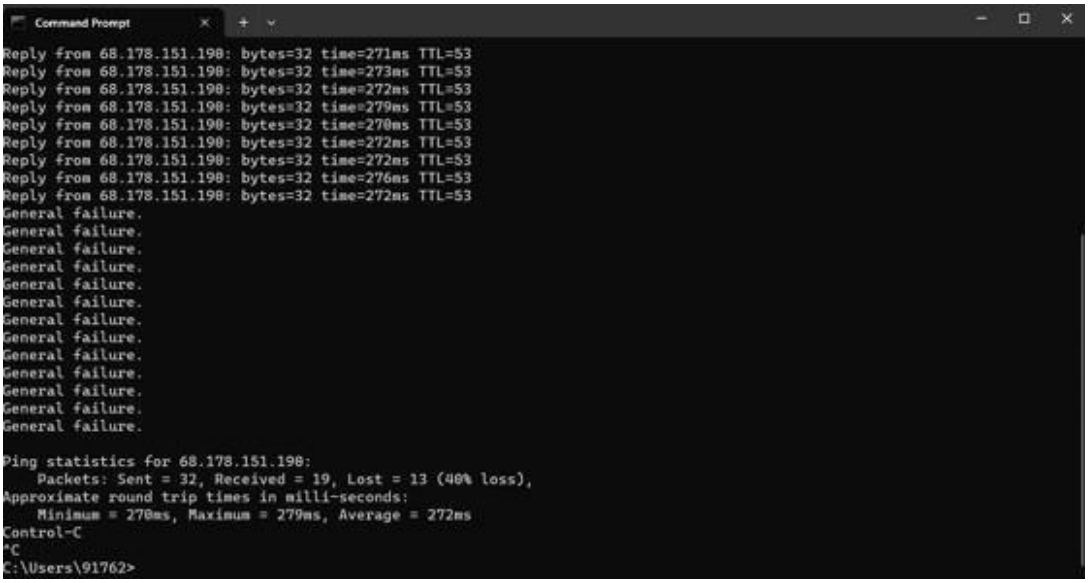
6.6 Blocking and Unblocking TCP and UDP rules

TCP inbound and outbound options, UDP inbound and outbound options so all services will not be blocked if you select inbound rule option for TCP it will block only inbound traffic in previous code both inbound and outbound traffic were blocked.


Protocol Blocker
Select protocols to block:
TCP Inbound
TCP Outbound
UDP Inbound
UDP Outbound
Block Selected

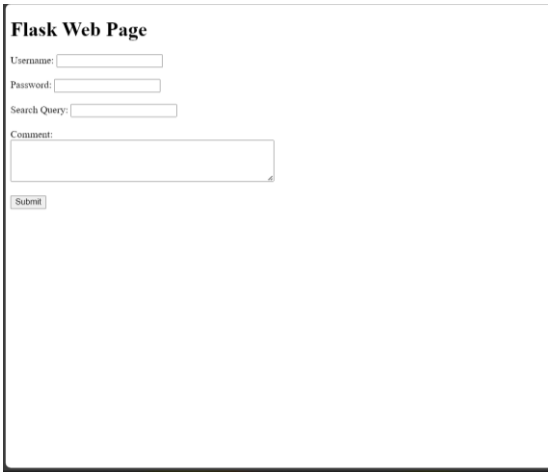

YouTube
Search
Home
Shorts
Subscriptions
You
Your channel
History
Your videos
Watch Later
Your clips
Show more
Subscriptions
Sony SAB
K18
Connect to the Internet
You're offline. Check your connection.
Retry
No Internet connection





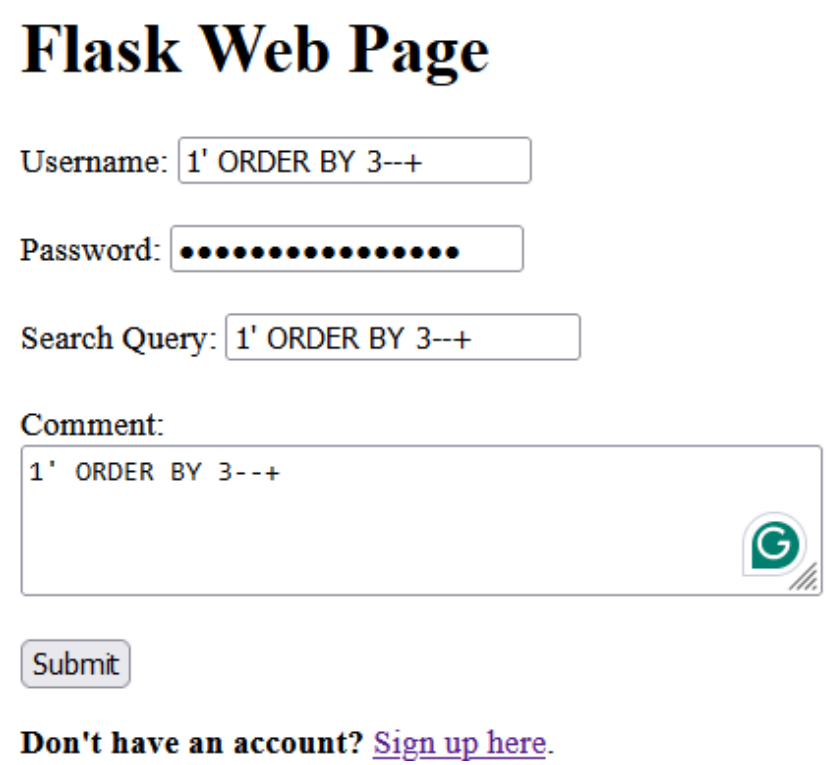
While running the script I was pinging a website it was showing error in sending ICMP packets due the blocked traffic of ICMP inbound and outbound rule.

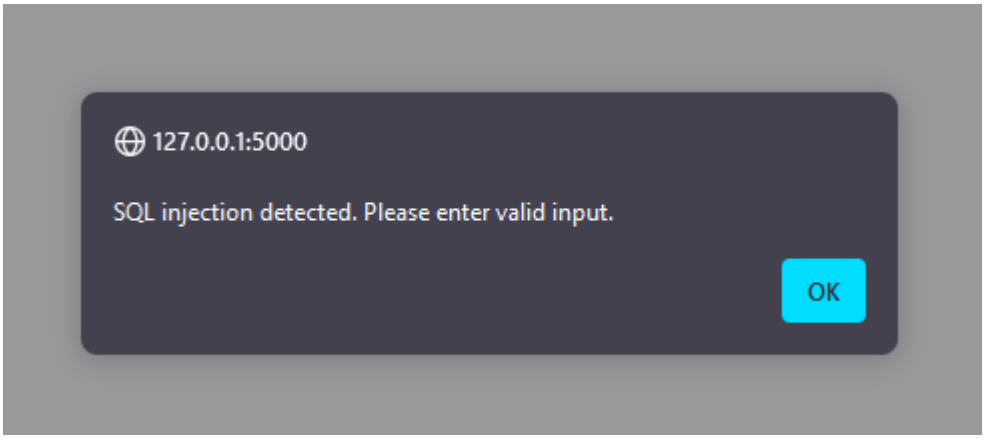
6.7 Made local web page in flask



This our local web page designed in flask this web page is connected to database and made for testing purpose like we tried different attacks on this web page and through our WAF we try to filter out the attacks payloads and blocked them.

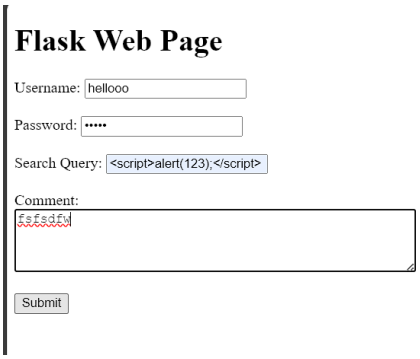
6.8 Filtration of SQL Payloads on web page

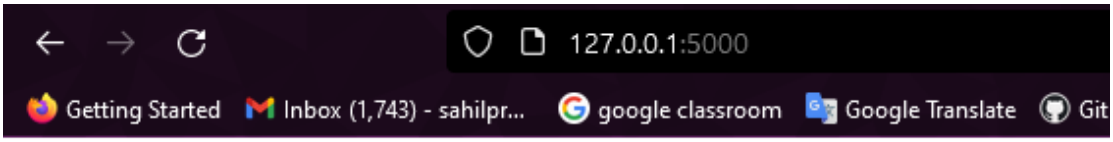




Script will detect the SQL injection payload and not allowed the inputted data to store in database.

6.9 Filtration of XSS payloads on web page

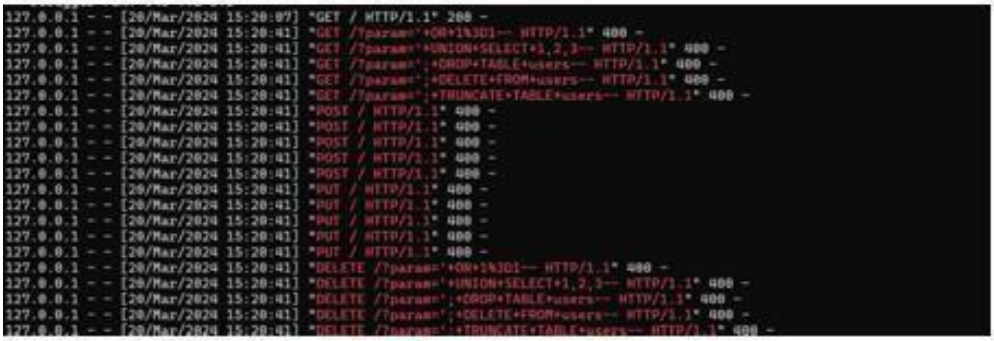




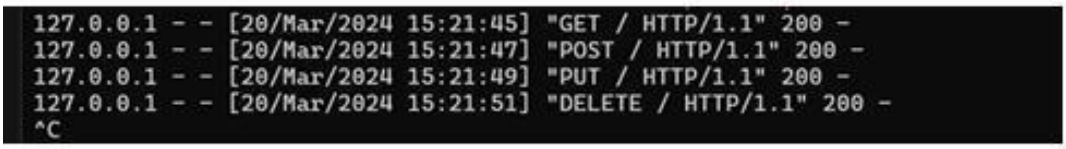
Method Not Allowed

The method is not allowed for the requested URL.

6.10 Filter malicious request sent in different methods



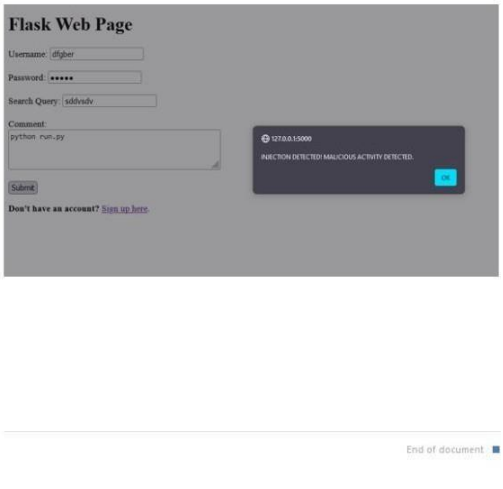
Blocking Sql Parameters Requests



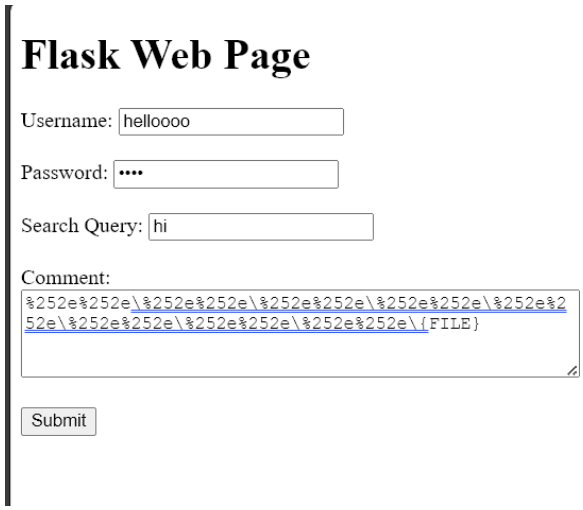
Allowing Normal Requests

This will filter out request sending attached SQL injection parameters through four different types of methods like GET, POST, PUT, DELETE filtration script will filter out all the requests which has SQL injection parameters and it will allow normal request and send back response “Welcome to Home Page”.

6.11 Filtration of OS command injection on web page



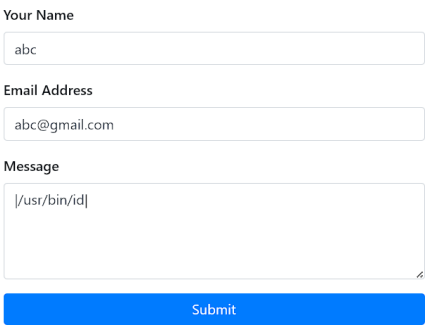
6.12 Filtration of Path traversal payload on web page

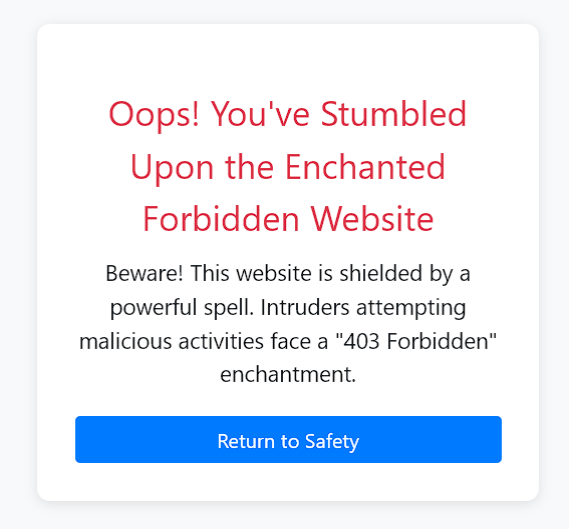


Potential path traversal detected. Please enter valid text.

6.13 Filtration of Linux based command payload on web page

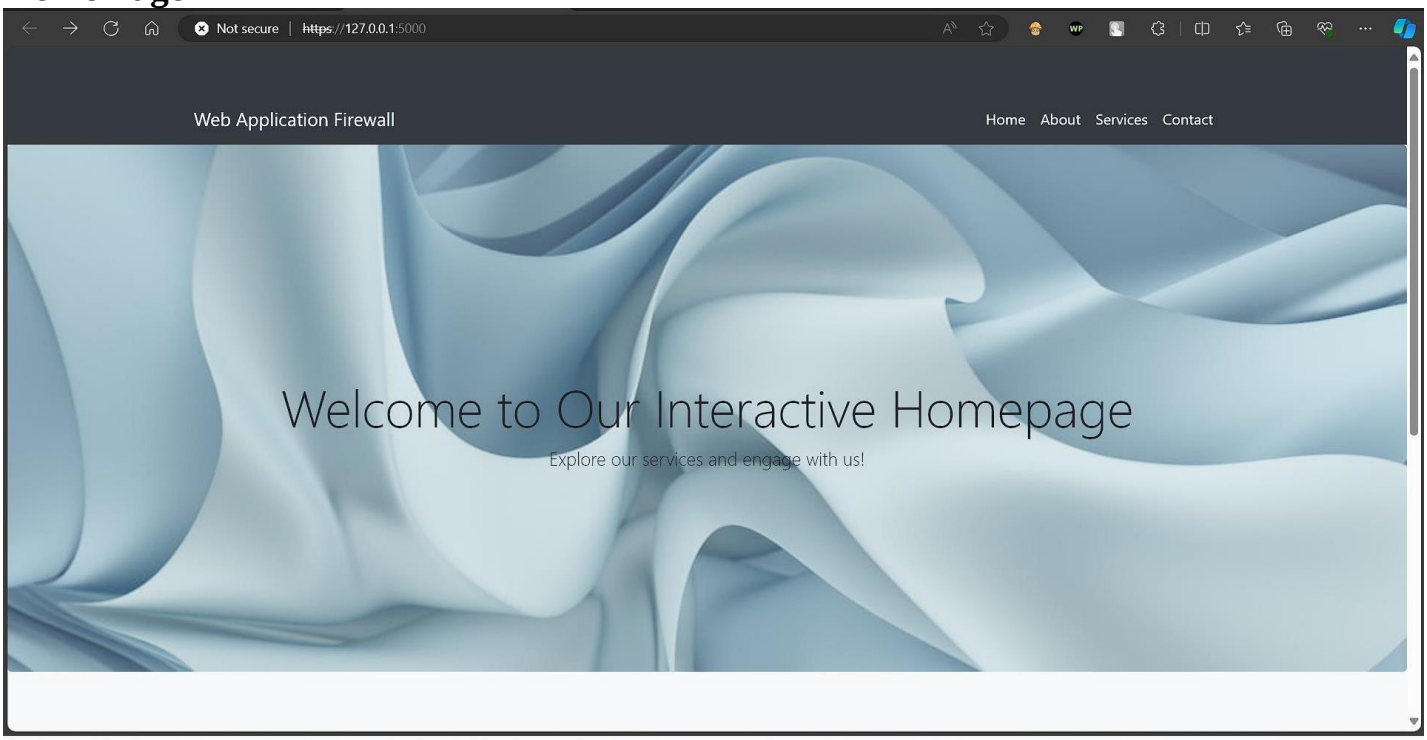
Entering command-based payload in our web page but as we click on submit it will block it and shows us malicious activity captured message.

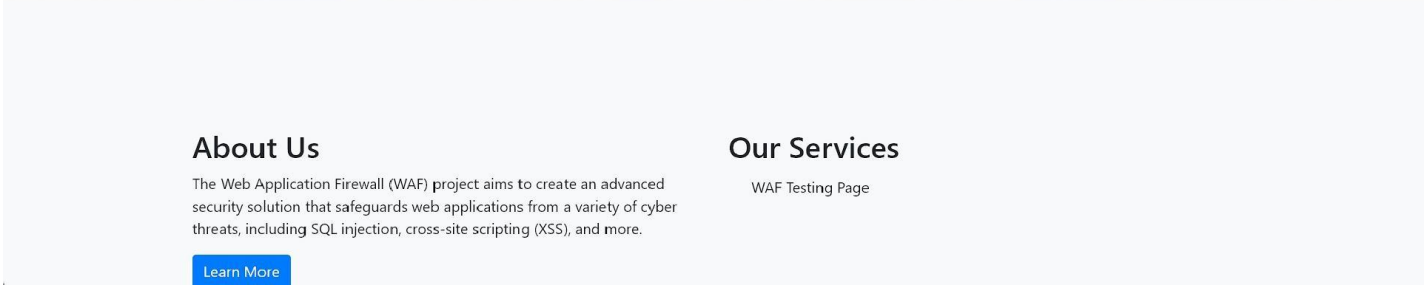




6.14 Created UI\UX design of our web page

Home Page





ABOUT US PAGE

Hello!!

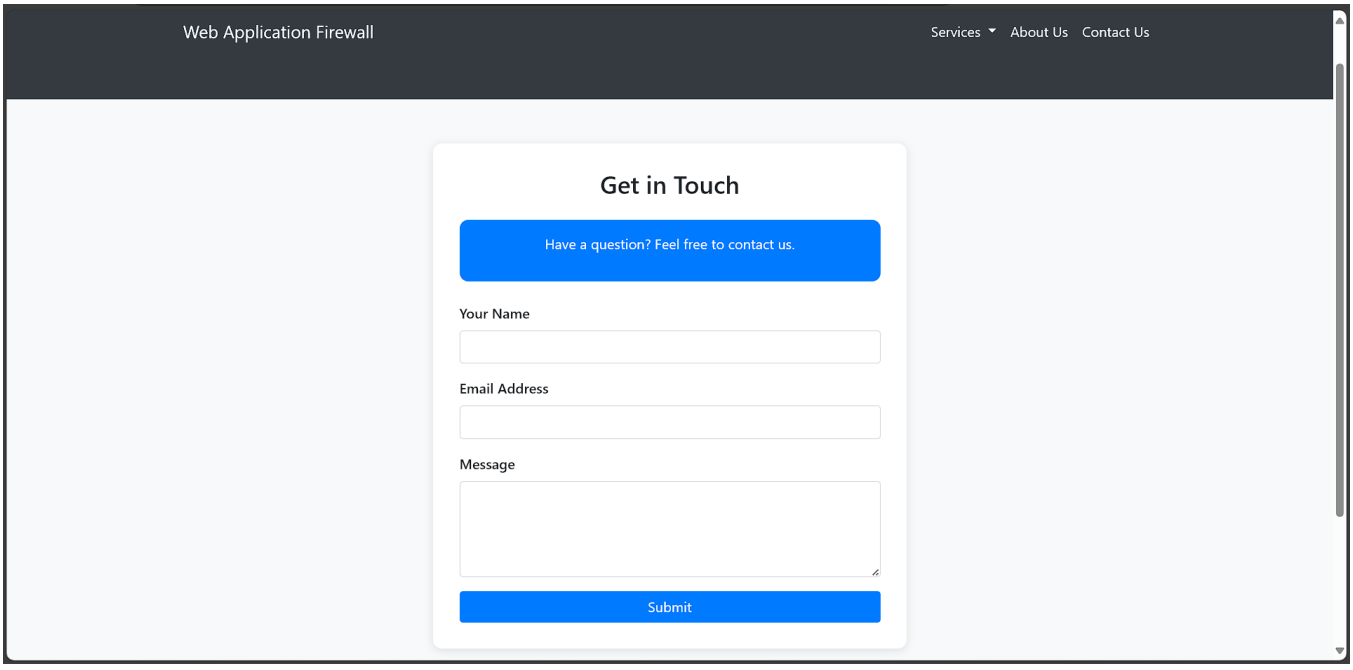
About Me

Urmik Pandya!

Project Details - WAF

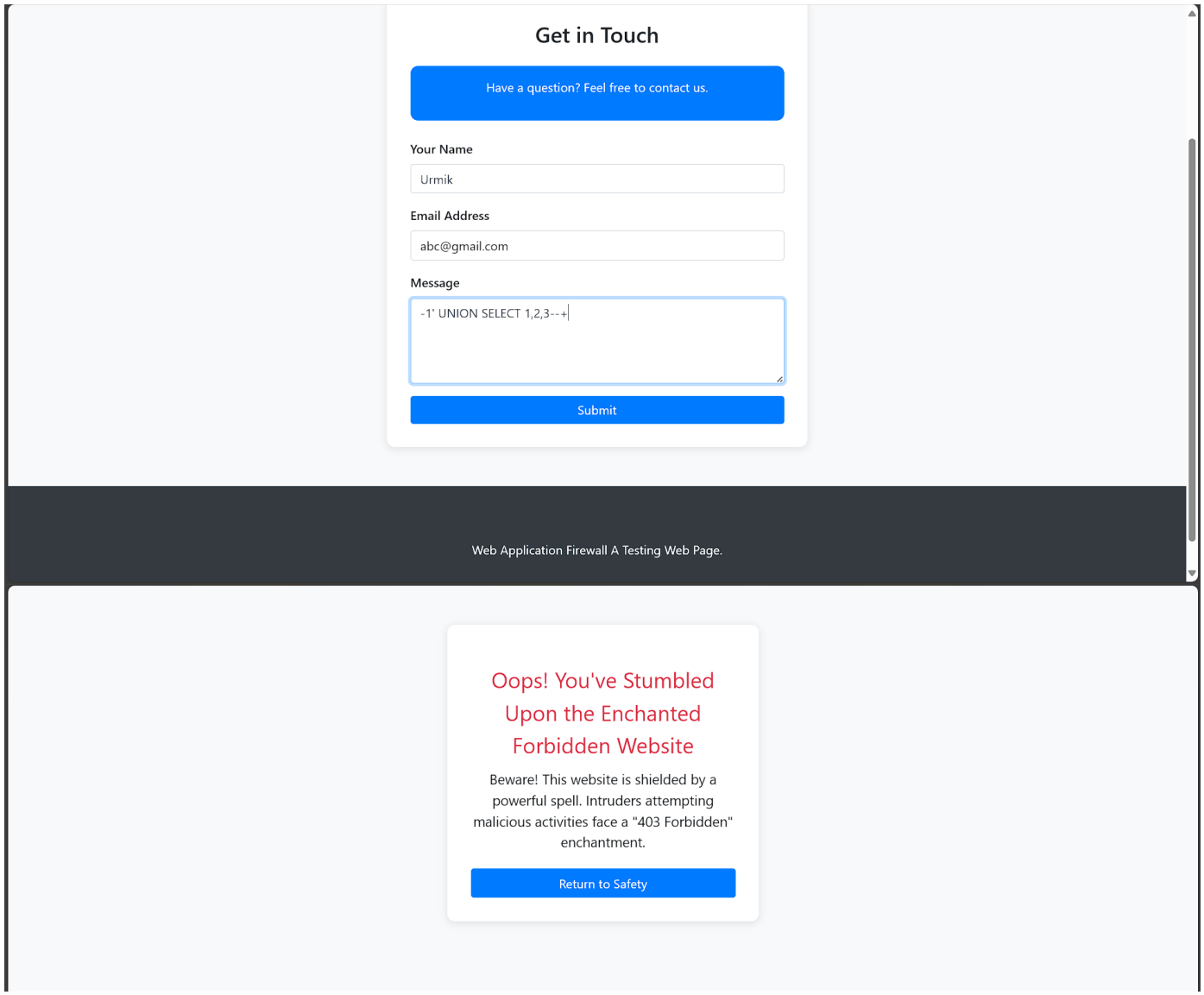
The Web Application Firewall (WAF) project aims to create an advanced security solution that safeguards web applications from a variety of cyber threats, including SQL injection, cross-site scripting (XSS), and more. By implementing intelligent traffic filtering and anomaly detection techniques, the WAF ensures that only legitimate and safe traffic reaches the application server.

CONTACT US PAGE

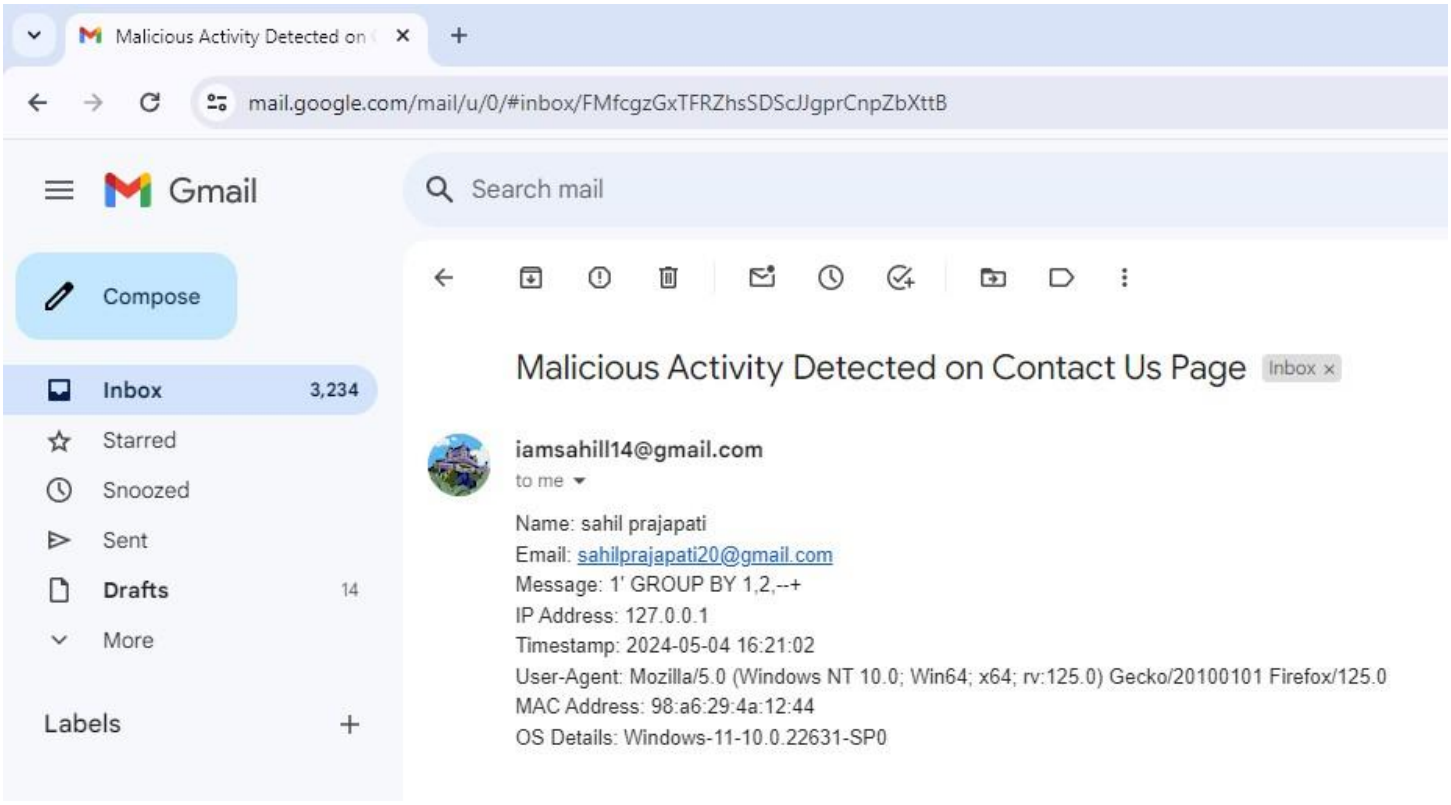


6.15 Capturing and Blocking Malicious Payload

Basically this function will block all the malicious payloads which are being entered by any hacker or a person with corrupt mind who is trying to get information by performing attacks on our webpage and our firewall will analyze and will capture any payload being entered on our webpage in this contact us page.

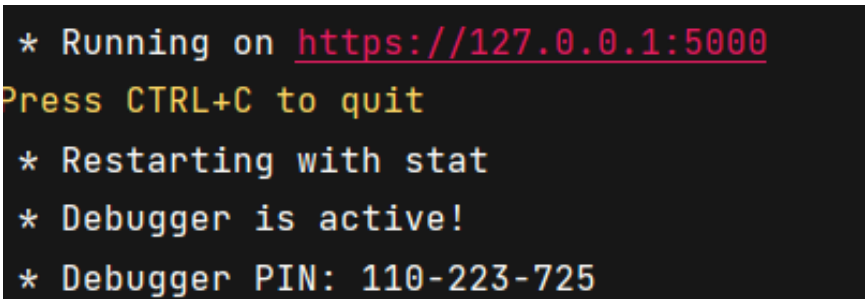


6.16 Sending mail when any malicious activity was captured



6.16 Added SSL certificate to our web page for security

We have added self-signed SSL certificate to our webpage to provide more security instead of http now local web page link will generate with Https.



CHAPTER: 7 CONCLUSION AND FUTURE WORK

CHAPTER 7 CONCLUSION AND FUTURE WORK

Future work

Looking ahead, future work in the realm of network-based firewall implementation involves continuous enhancements and adaptations to keep pace with evolving cyber threats and technological advancements. This includes staying abreast of emerging attack vectors, vulnerabilities, and regulatory requirements to ensure the ongoing effectiveness of the firewall solution. Additionally, there is a need to explore and integrate innovative security technologies such as artificial intelligence (AI) and machine learning (ML) to enhance threat detection capabilities and automate response mechanisms. Moreover, as organizations increasingly embrace cloud computing and distributed architectures, there will be a growing focus on implementing cloud-native firewall solutions and leveraging technologies like micro-segmentation to secure dynamic and decentralized networks effectively. Collaboration with industry peers, participation in threat intelligence sharing initiatives, and engagement with cyber security research communities will also be pivotal in shaping future strategies for network security and firewall management. Ultimately, the continuous refinement and evolution of network-based firewall implementations will be essential to safeguarding critical assets, preserving data integrity, and ensuring the resilience of organizational networks against emerging cyber threats.

CONCLUSION

Web Application Firewalls (WAFs) and network firewalls are indispensable components of modern cyber security strategies, each playing a crucial role in protecting against different types of threats. WAFs excel in safeguarding web applications from application-layer attacks, offering granular control and deep inspection of HTTP/HTTPS traffic. On the other hand, network firewalls provide broader network-level protection by regulating traffic flow based on network-layer parameters such as IP addresses and ports. Future work in this field should focus on enhancing integration and collaboration between these technologies, advancing threat detection capabilities, developing cloud-native solutions, leveraging automation and orchestration, and incorporating Zero Trust principles. By addressing these areas, organizations can fortify their defenses and adapt to the evolving threat landscape effectively.

CHAPTER: 8 REFERENCES

CHAPTER 8 REFERENCES

- www.google.com
- www.youtube.com
- www.geeksforgeeks.com
- www.fortinet.com
- www.researchgate.com
- http://www.securityfocus.com/infocus/1716
- http://www.securityfocus.com/infocus/1817
- https://www.techtarget.com/searchapparchitecture/tip/XML-Firewalls
- https://www.sei.cmu.edu/about/divisions/cert/index.cfm