



GROUP 8

Dec 03, 2023

PROJECT-SECURITY TESTING REPORT

ISMAIL MAHAMED 125052191

JASKARAN SOHAL 150343218

RAYYAN KHAN 155534209

EASTON SOARES 108851213

Table of Contents

Executive Summary	4
Testing Scope:	4
SQL Injection Testing using SQLMap:	5
Zap Proxy - Security Testing on Corporate Site Container:	5
Pi Hole Security Assessment	7
Nikto Tool - Testing DHCP and Private DNS Machine:	7
Fuzzing - Network Services:	8
HTTPS – SSL encryption	9
IDS – Snort Detection Logs	10
Recommendations	10

Figure 1: SQL injection.....	5
Figure 2: SQL injection WAF	5
Figure 3: Zaproxy Corp site.....	6
Figure 4:Nmap Port Scanning.....	7
Figure 5: Nikto on DHCP Machine & DNS Machine	7
Figure 6: Nikto Corpsite	7
Figure 7: Wfuzz DHCP & DNS machine	8
Figure 8: Wfuzz Corpsite.....	8
Figure 9: Wfuzz Ecom site.....	8

Executive Summary

This security testing report provides a thorough examination of the security features embedded within the network topology of Binary Stream. The primary objective of this evaluation is to assess the effectiveness of the security measures in place. The network comprises 10 devices, featuring two routers—a core router dedicated to internal services and an external router. The core router assumes a pivotal role by hosting indispensable services, such as a Public Key Infrastructure (PKI) certificate. Additionally, it is equipped with an internal firewall that incorporates advanced security features, including an Intrusion Detection System (IDS) and OpenVPN.

THE DEVICES ARE STRATEGICALLY SEGMENTED INTO DISTINCT ZONES TO FORTIFY SECURITY MEASURES:

MANAGEMENT ZONE

Management Zone Devices:
Network Services
Private DNS
Active Directory

Table 1: Management Zone

DEMILITARIZED ZONE

Docker containers hosting web servers for the workplace
Dedicated machine for hosting web servers within a Docker container

Table 2: DMZ

INTERNAL ZONE

Internal Zone:
User
Admin
Remote User

Table 3: Internal Zone

Testing Scope:

The security testing covered various facets of the topology, with a specific focus on the following key areas:

NETWORK SERVICES SECURITY:

Analysis of network configurations and protocols to ensure resilience against unauthorized access.

Core Router Security:

Thorough examination of PKI certificate implementation.

Assessment of the effectiveness of the internal firewall, IDS, and SSL encryptions.

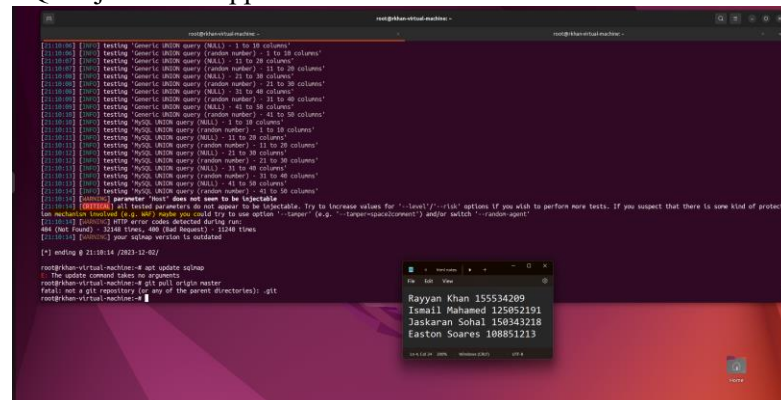
DMZ Security:

Evaluation of the dedicated machine's security within the Docker container environment.

in our effort to assess network security, we conducted SQL injection testing using SQLMap from an external connection. This simulated attack aimed to gauge our system's susceptibility to SQL injection threats. Utilizing SQLMap, we sought to evaluate the effectiveness of our defenses, particularly our Web Application Firewall (WAF), in preventing unauthorized access and potential data breaches.

[illegible]

SQL injections stopped due to WAF



Despite attempts to inject SQL queries, our Web Application Firewall (WAF) effectively thwarted these efforts, demonstrating its efficacy in preventing unauthorized access and potential data breaches.

We employed Zaproxy as the tool of choice for conducting a security assessment on the corporate site container.

Testing the Corpsite Container

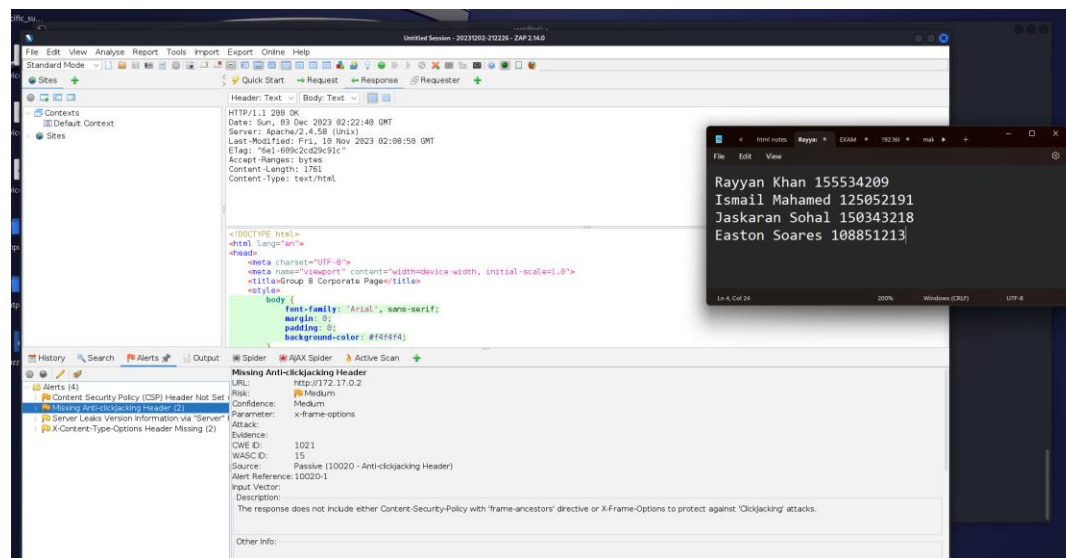


Figure 3: Zapproxy Corpsite

Testing Ecom Webserver Container

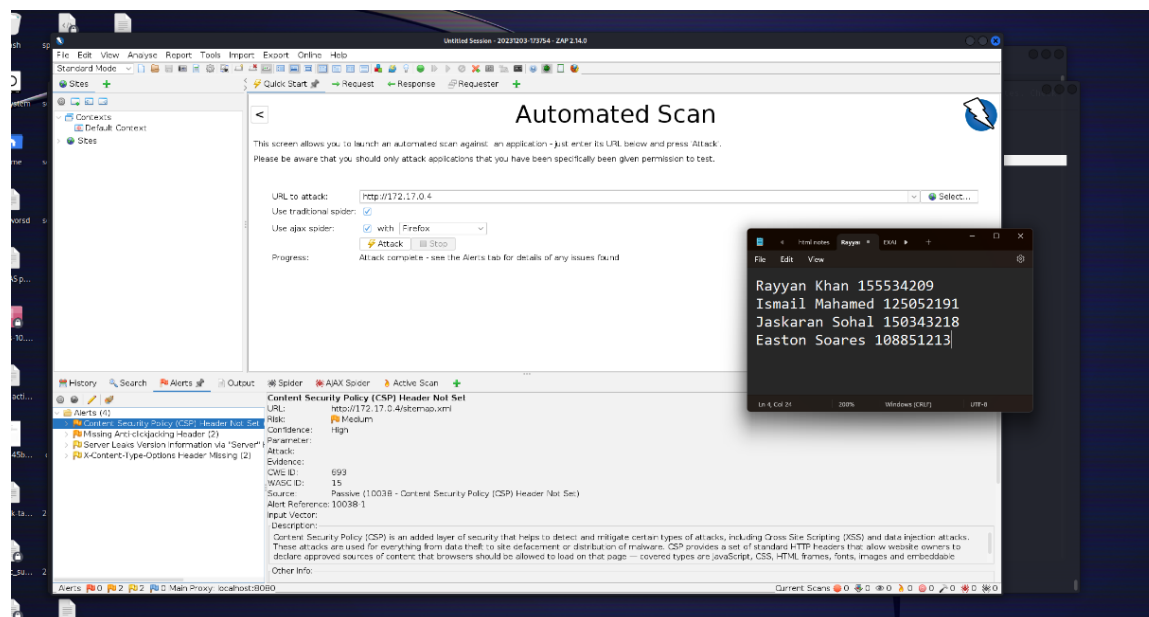


Table 4: zapproxy Ecom Site

The examination of our corporate site container using Zap Proxy revealed a reassuring outcome. No critical issues requiring immediate attention were identified. While the tool generated alerts, they were deemed insignificant, posing no real threat to the container's security. The alerts, although numerous, were largely out of scale and didn't introduce vulnerabilities that could harm the container.

Pi Hole Security Assessment

In this segment of the assignment, we utilized the tool Nmap for port scanning purposes.

Nmap Testing:



Figure 4:Nmap Port Scanning

The scan on the Pi Hole revealed an open port and visible service to the scanning machine. To enhance security, it is recommended to close this port to prevent external visibility. This precautionary measure will bolster the overall security posture, minimizing the risk of unauthorized access.

Nikto Tool - Testing DHCP and Private DNS Machine:

In this section of the assignment, we employed the Nikto tool to unveil information about the DHCP and Private DNS machine.

Nikto Tool:

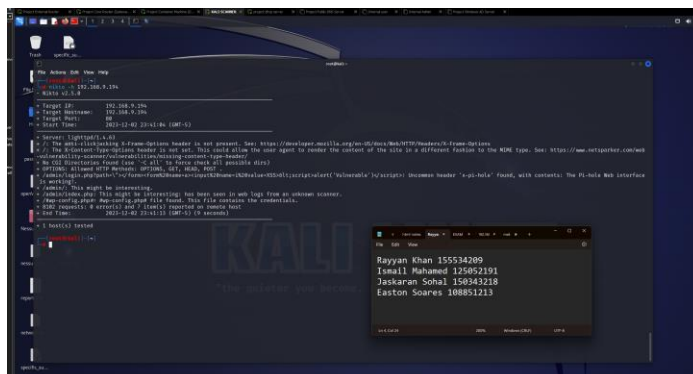


Figure 5: Nikto on DHCP Machine & DNS Machine

Nikto on Corpsite:



Figure 6: Nikto Corpsite

Nikto scans on the DHCP and Private DNS machine uncovered noteworthy information about the web server's security and configuration. Identified concerns include the absence of "X-Frame-Options" and "X-Content-Type-Options" headers, potentially exposing the site to clickjacking and MIME-sniffing attacks. Further investigation into the absence of CGI directories is advised, along with addressing potentially sensitive paths. These findings underline the need for administrators to address vulnerabilities and enhance overall security measures.

Fuzzing - Network Services:

In this segment of the assignment, we employed the tool known as wfuzz to initiate the process of fuzzing across all network services.

Wfuzz on the Network Services and private dns

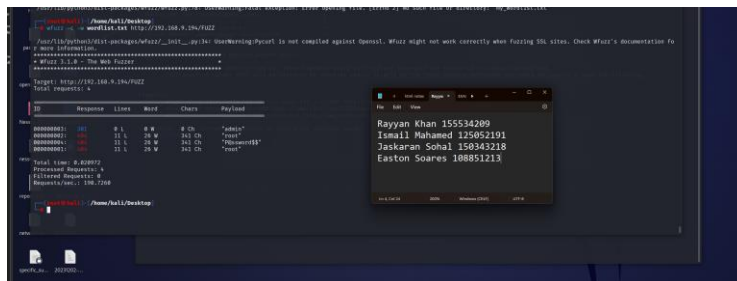


Figure 7: Wfuzz DHCP & DNS machine

Corpsite

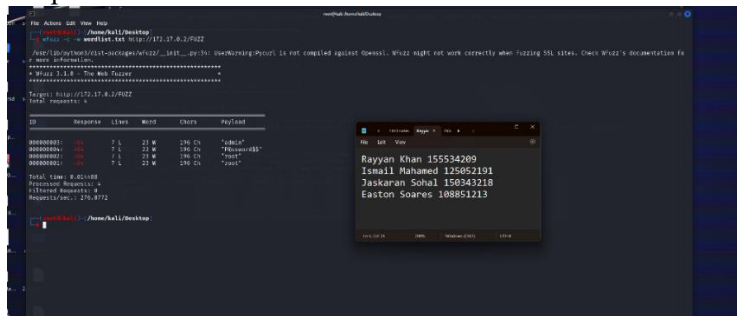


Figure 8: Wfuzz Corpsite

Ecom site fuzzing:

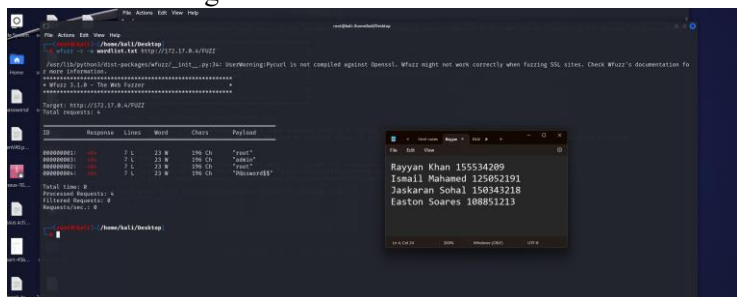


Figure 9: Wfuzz Ecom site

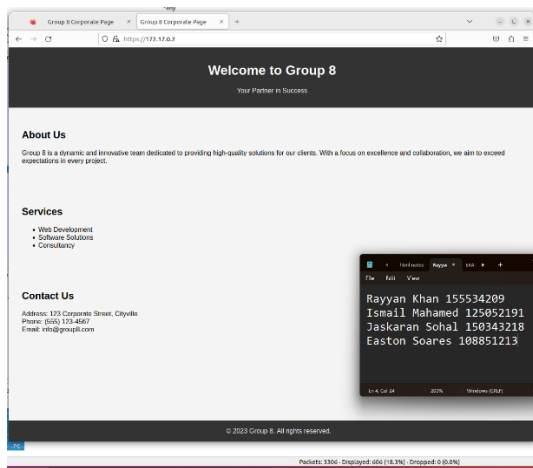
Fuzzing tests on the network services and DHCP machine revealed that the HTTP TRACE method is present, potentially exposing the system to Cross-Site Tracing (XST) attacks. Administrators are advised to investigate the necessity of this method and disable it if not required to mitigate the associated risk.

HTTPS – SSL encryption

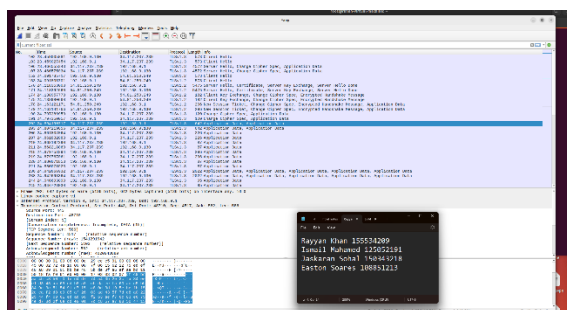
Within our topology, we integrated the use of SSL encryption for our web servers to secure the information exchanged between users and the server.

The objective was to implement SSL (Secure Sockets Layer) encryption, which secures the transmission of information between users and web servers by encrypting the data. This makes it considerably more difficult for unauthorized entities to intercept and decipher the transmitted data. SSL encryption establishes a secure and private communication channel, offering protection to sensitive information like login credentials.

SSL Site:



Wireshark analysis:



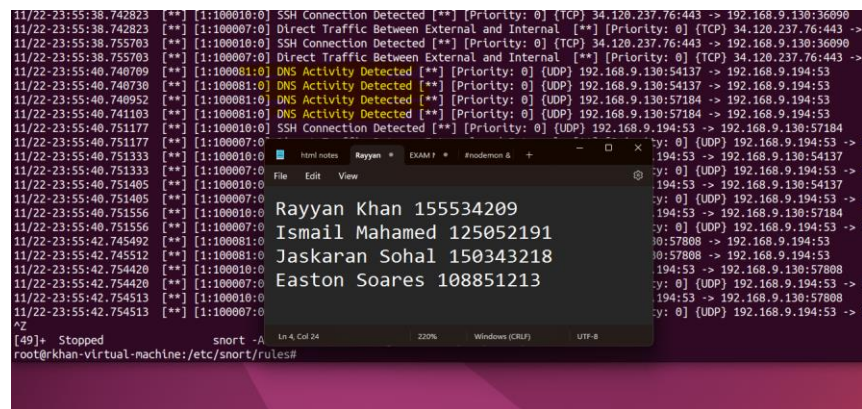
Upon analyzing the Wireshark data above, it is apparent that encryption measures are in place during the communication between the client and the server. The encrypted nature of the data signifies a

commitment to securing the transmitted information. However, the specifics of the content remain indecipherable within the Wireshark analysis due to the protective encryption layer.

IDS – Snort Detection Logs

We have implemented the tool called Snort into our network infrastructure to function as our Intrusion Detection System (IDS), primarily designed to identify and alert on unwanted connections and potential threats. Snort acts as a robust intrusion detection tool, continuously monitoring network traffic for suspicious patterns and known signatures associated with various cyber threats. This proactive approach enables us to promptly detect and respond to potential security incidents.

Snort logs:



The screenshot displays a terminal window with a dark background. The top portion shows a series of Snort log entries in a monospaced font, including timestamps, rule IDs, and event descriptions such as 'SSH Connection Detected' and 'DNS Activity Detected'. Overlaid on the terminal is a semi-transparent window titled 'Hosts' containing a list of IP addresses and names: Rayyan Khan 155534209, Ismail Mahamed 125052191, Jaskaran Sohal 150343218, and Easton Soares 108851213. The bottom of the terminal shows the command prompt 'root@khan-virtual-machine: /etc/snort/rules#'.

The screenshot above shows a plethora of logs collected by snort. The rules outlined above play a pivotal role in adopting a proactive stance against undesirable activities and suspicious behaviors. By leveraging these rules, we strengthen our ability to identify and respond to potential security threats swiftly, ensuring a vigilant and robust defense against unauthorized actions within our network.

Recommendations

The security testing report has illuminated key areas of strength and areas warranting improvement within the Binary Stream network topology. To fortify the network's security posture, we recommend implementing the following mitigation strategies:

WAF Optimization:

Given the successful defense against SQL injection attempts by the Web Application Firewall (WAF), ongoing optimization is crucial. Regular updates and fine-tuning of WAF rules are recommended to adapt to evolving threats and maintain a robust defense mechanism.

Container Security Best Practices:

While the corporate site container demonstrated resilience against potential threats during Zap Proxy testing, a proactive approach involves adhering to container security best practices. Regular security audits, patch management, and continuous monitoring can ensure the container remains secure over time.

Pi Hole Port Closure:

The identification of an open port on the Pi Hole during Nmap testing suggests a potential vulnerability. To mitigate this risk, it is imperative to close the open port to prevent external visibility. This preventive measure contributes to minimizing the risk of unauthorized access and enhancing overall security.

Web Server Security Enhancements:

Nikto scans on the DHCP and Private DNS machine revealed security concerns, such as the absence of critical headers. Administrators should promptly implement missing security headers, investigate the absence of CGI directories, and address potentially sensitive paths. These measures collectively enhance the overall security of web servers and mitigate potential vulnerabilities.

HTTP TRACE Method Mitigation:

Fuzzing tests identified the presence of the HTTP TRACE method on the network services and DHCP machine, posing a potential risk of Cross-Site Tracing attacks. Administrators are advised to thoroughly investigate the necessity of this method and, if not required, disable it to mitigate the associated risk effectively.

Continuous Security Training:

In tandem with technical measures, investing in continuous security awareness training for employees is essential. This ensures that the human factor remains vigilant against social engineering and other non-technical threats.

Implementing these mitigation strategies will contribute to an overall enhanced security posture for the Binary Stream network, fortifying defenses against potential threats and ensuring the longevity of a secure environment. Regular reviews and updates will further optimize security measures based on emerging threats and evolving best practices.