**Penetration Testing Report**

**1. Executive Summary**

This report details a penetration test conducted on two target applications, https://canarabank.com and https://lanes-deserve-wholesale-n.trycloudflare.com, which revealed multiple security issues related to **Broken Authentication** and **Broken Access Control**. These vulnerabilities could allow unauthorized access to sensitive functionalities or data if exploited. Immediate steps are required to address these weaknesses and improve the overall security posture.

**Key Findings:**

* **Target 1 (https://canarabank.com):**
  + Good security practices observed; no critical issues detected.
* **Target 2 (https://lanes-deserve-wholesale-n.trycloudflare.com):**
  + Missing critical security headers.
  + Open ports expose potential attack surfaces.

**Severity**: Moderate (Target 1) | High (Target 2)

**2. Scope of Work**

**Objectives:**

1. Identify vulnerabilities related to authentication mechanisms and access control.
2. Evaluate the effectiveness of security headers and open ports.
3. Provide actionable recommendations to mitigate risks.

**Tools Used:**

* Kali Linux
* Nmap
* Python Scripts (Custom scanning tools)
* Browser Developer Tools

**3. Methodology**

The following steps were followed during the penetration testing process:

**3.1 Reconnaissance**

* Verified both target applications were reachable.
* Identified input fields and analyzed their behavior for vulnerabilities.

**3.2 Port Scanning**

* Conducted port scanning using Python's socket library and Nmap.
* Checked for open ports and recorded their services.

**3.3 Application Information Gathering**

* Sent HTTP/HTTPS requests to identify server headers and security configurations.
* Extracted the following information:
  + Server Type (via HTTP headers).
  + Presence of security headers (CSP, HSTS, X-XSS-Protection, etc.).

**3.4 Vulnerability Analysis**

* Analyzed the security posture of both applications based on open ports and missing security headers.

**4. Test Results**

**Target 1: https://canarabank.com**

* **Web Application Firewall (WAF):** Detected BIG-IP AppSec Manager (F5 Networks).
* **HTTP Headers:** Security headers implemented include:
  + Cache-Control
  + Content-Type
  + X-Content-Type-Options
  + X-XSS-Protection
  + X-Frame-Options
  + Referrer-Policy
  + Content Security Policy (CSP)
  + HTTP Strict Transport Security (HSTS)
* **Open Ports:**
  + 80/tcp (HTTP)
  + 443/tcp (HTTPS)
* **Outdated CMS:** No content management system (CMS) detected.
* **Website Safety:** Demonstrates good security practices with no critical issues identified.

**Target 2: https://lanes-deserve-wholesale-n.trycloudflare.com**

* **Web Application Firewall (WAF):** Unable to verify WAF due to connection timeout.
* **HTTP Headers:** Missing critical security headers, including:
  + Content Security Policy (CSP)
  + HTTP Strict Transport Security (HSTS)
  + X-Frame-Options
  + X-XSS-Protection
* **Open Ports:**
  + 80/tcp
  + 443/tcp
  + 8080/tcp
  + 8443/tcp
* **Outdated CMS:** No CMS detected.
* **Website Safety:** Lacks essential security configurations. Potential attack surfaces include open ports and missing headers.

**5. Recommendations**

To improve the security posture of the tested applications, the following steps are recommended:

**5.1 Implement Web Application Firewall (WAF)**

* Verify and configure WAF settings to block malicious traffic effectively.
* Test the WAF to ensure it can detect and mitigate common attacks (e.g., SQL Injection, XSS).

**5.2 Enforce Security Headers**

* Implement the following HTTP security headers:
  + **Content Security Policy (CSP):** Prevents injection attacks by restricting resource loading.
  + **HTTP Strict Transport Security (HSTS):** Ensures secure HTTPS connections.
  + **X-Frame-Options:** Prevents clickjacking attacks.
  + **X-XSS-Protection:** Protects against reflected XSS attacks.

**5.3 Secure Open Ports**

* Conduct regular port audits to ensure only necessary ports are open.
* Restrict access to sensitive ports using firewalls and IP whitelisting.

**5.4 Monitor and Update Configurations**

* Continuously monitor application behavior and server configurations for anomalies.
* Ensure timely updates to servers, frameworks, and dependencies.

**6. Conclusion**

The penetration test revealed varying security postures between the two target applications:

1. **https://canarabank.com** demonstrates strong security practices, with no critical vulnerabilities detected.
2. **https://lanes-deserve-wholesale-n.trycloudflare.com** requires significant improvements, including the implementation of security headers and securing open ports to mitigate potential risks.

**Summary:**

* **Target 1:** Secure with minor observations.
* **Target 2:** Vulnerable due to missing headers and exposed ports.
* **Recommendations:** Implement security headers, configure WAF, and audit open ports.