1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **snacks.com** using a Basic analysis methodology. The evaluation commenced on **June 24th at 15:45** and concluded after a duration of **1 hour, 32 minutes, and 36 seconds**. The scope of the analysis included a comprehensive review of web applications and infrastructure, focusing on identifying high and medium-risk vulnerabilities.

1.2 Short Summary of Main Issues

The assessment identified **3 high-risk** and **4 medium-risk** issues. The most critical finding is the exposure of **43 email addresses and passwords** on the deep web, posing significant risks of phishing attacks and unauthorized access. Unusual port assignments and open FTP services were detected, indicating potential misconfigurations. Additionally, a high service density on a single host increases the attack surface, with **8 services** vulnerable to brute force attacks.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked	High
Unusual Port Assignments Detected	High
FTP Service	High
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
Services Vulnerable to Brute Force Attacks	Medium
Login Form Detection Analysis	Medium

1.4 Email Addresses and/or Passwords Leaked on the Deep Web

Description:
A total of **43 email addresses and passwords** were found leaked on the deep web. This exposure poses critical security risks, including unauthorized access, phishing attacks, social engineering, and further data breaches. The credentials were sourced from multiple databases such as AntiPublic and BreachCompilation.

Affected Assets:
- Email addresses and passwords of the organization.

Recommendations:
Immediate actions should include notifying affected users, enforcing password changes, implementing multi-factor authentication, and monitoring for suspicious activities. Additionally, employee training on recognizing phishing attempts should be prioritized.

1.5 Unusual Port Assignments Detected

Description:
A total of **16 unusual port assignments** were identified, with **2 high-risk assignments**. Services

are running on non-standard ports or ports running unexpected services, which may indicate attempts to evade detection or misconfigured applications.

Affected Assets:

- Host: **snacks.com** and **www.snacks.com** with IP **45.223.17.132**.

Recommendations:

Review and reconfigure port assignments to align with standard practices. Implement firewall rules to restrict access to necessary ports only and conduct regular audits to ensure compliance with security policies.

1.6 FTP Service

Description:

An open FTP port was detected, which can lead to unauthorized access, malicious file uploads, website defacement, denial of service attacks, interception of cleartext traffic, exploitation of FTP server vulnerabilities, and brute-force attacks.

Affected Assets:

- IP Address: **45.223.17.132** - Host: **www.snacks.com**

Recommendations:

Disable FTP services if not required or replace them with secure alternatives like SFTP or FTPS. Ensure strong authentication mechanisms are in place and monitor for any unauthorized access attempts.

1.7 Nmap Port Scan Results Analysis

Description:

The scan revealed **108 open ports**, with several associated with potentially insecure services or protocols. These vulnerabilities could lead to unauthorized access, data interception, and other security breaches.

Affected Assets:

- Complete Nmap scan results are available in the downloads section.

Recommendations:

Conduct a thorough review of open ports and associated services. Close unnecessary ports and ensure that remaining services are securely configured. Regularly update software to patch known vulnerabilities.

1.8 Service Density Analysis

Description:

A high service density was detected on a single host with **30 services**, increasing the attack surface. Specific ports were marked as potentially insecure.

Affected Assets:

- Host IP: **45.223.17.132**

Recommendations:

Evaluate the necessity of each service running on the host and reduce the number where possible. Implement network segmentation to limit exposure and enhance monitoring for unusual activities.

1.9 Services Vulnerable to Brute Force Attacks

Description:
A total of **8 services** were identified as vulnerable to brute force attacks due to lack of account lockout mechanisms and weak password policies.

Affected Assets:
- IP Address: **45.223.17.132**

Recommendations:
Implement account lockout policies and rate limiting on authentication attempts. Strengthen password policies by enforcing complexity requirements and regular password changes.

1.10 Login Form Detection Analysis

Description:
Four login forms were detected across the application, indicating potential authentication interfaces requiring security validation.

Affected Assets:
- URLs include: - https://snacks.com/resetpassword/ - https://snacks.com:2121/createAccount - https://www.snacks.com/createAccount - https://snacks.com:8009/robots.txt?_AMP_safari_preconnect_polyfill_cachebust= - https://www.snacks.com/my-account/my-addresses

Recommendations:
Ensure all login forms are protected with HTTPS and implement CAPTCHA mechanisms to prevent automated attacks. Regularly test for vulnerabilities such as SQL injection or cross-site scripting (XSS).

1.11 General Recommendations

To enhance overall security posture, it is recommended to establish a comprehensive security policy that includes regular vulnerability assessments, employee training programs, incident response planning, and continuous monitoring of network activities. Implementing these measures will help mitigate risks and protect organizational assets from potential threats.