1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **flexuat2.keystonefunding.com**. The engagement commenced on **November 3rd** at **07:00** and concluded in a duration of **00 hours, 09 minutes, and 47 seconds**. The analysis was performed as a **Basic** scan. The primary objective was to identify High and Medium-risk vulnerabilities within the web application and its infrastructure using OWASP and OSCP methodologies.

1.2 Short Summary

The security assessment identified **17 issues**, with **1 High-risk** and **3 Medium-risk** findings. The most critical issue is the presence of **7 login forms**, posing a High risk due to potential unauthorized access. Medium-risk issues include insecure HTTP ports, sensitive subdomains, and an SSL certificate nearing expiration. Immediate remediation of these findings is crucial to mitigating potential security threats.

1.3 Key Security Issues

Title	Risk
Login Form Detection Analysis	High
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL Certificate Expiration Analysis	Medium

1.3.1 High-Risk Issue

Login Form Detection Analysis **Description:**
A total of **7 login forms** were detected across the application, indicating a High interest level due to the potential for unauthorized access. This finding includes multiple URLs where login forms are present, increasing the attack surface for credential-based attacks.

Affected Assets:
- URLs with detected login forms: - `https://flexuat2.keystonefunding.com/index` - `https://flexuat2.keystonefunding.com/loan` - `https://flexuat2.keystonefunding.com/02/29` - `https://flexuat2.keystonefunding.com/privacy_statement` - `https://flexuat2.keystonefunding.com:443` - `https://flexuat2.keystonefunding.com/login` - `https://flexuat2.keystonefunding.com/disclaimer` - `https://flexuat2.keystonefunding.com/forgotpassword` - `https://flexuat2.keystonefunding.com/having_trouble`

Recommendations:
Implement multi-factor authentication (MFA) to enhance login security. Regularly audit login endpoints to ensure they are protected against brute-force attacks. Employ rate limiting and CAPTCHA mechanisms to mitigate automated attack attempts.

1.3.2 Medium-Risk Issues

Nmap Port Scan Results Analysis **Description:**
The scan detected **2 open ports**, including port **80/tcp** associated with HTTP service, which lacks encryption. This could expose sensitive data if not properly redirected to HTTPS or protected by HSTS.

Affected Assets:
- IP: **66.6.16.168** with open ports **80/tcp** and **443/tcp**.

Recommendations:
Ensure that HTTP traffic is automatically redirected to HTTPS. Enable HSTS to enforce secure connections and prevent man-in-the-middle attacks.

Subdomain Naming Security Assessment Description:
A sensitive subdomain categorized as “Development/Staging” was identified, posing a Medium risk due to potential exposure of critical systems and data.

Affected Assets:
- Subdomain: **flexuat2.keystonefunding.com**

Recommendations:
Restrict access to development and staging environments from the public internet. Ensure these environments are regularly patched and do not expose sensitive information or administrative interfaces.

SSL Certificate Expiration Analysis Description:
The SSL/TLS certificate for the domain is set to expire in **37 days**, placing it in the warning category for certificate renewal.

Affected Assets:
- Domain: **flexuat2.keystonefunding.com**

Recommendations:
Initiate the renewal process for the SSL/TLS certificate promptly to avoid disruptions in secure communications. Implement monitoring solutions to alert on upcoming certificate expirations.

1.4 General Recommendations

To strengthen the overall security posture, it is recommended to implement a continuous security monitoring program, ensuring all identified vulnerabilities are addressed promptly. Regular updates and patches should be applied across all systems, and security awareness training should be conducted for staff to mitigate human-related risks.