1 Executive Security Assessment Report

1.1 Introduction

This report details the findings from a security assessment conducted on the domain **shinhan.fdecs.com**. The assessment was initiated on **May 26th** at **19:45** and completed in **00h:09m:36s**. The scope of the work involved a basic analysis focusing on identifying potential vulnerabilities within the web application and infrastructure, utilizing methodologies from OWASP and OSCP.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High, **1** Medium, **1** Low, and **16** informational. The most significant finding is the Medium-risk issue related to open port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS. This could expose sensitive data to interception, impacting business confidentiality. Additionally, the Low-risk finding highlights the absence of modern TLS 1.3 support, which could affect data integrity and security. Despite these concerns, the assessment shows no evidence of shared hosting environments, high-risk geographic server locations, or services vulnerable to brute force attacks. It is recommended to address the Medium-risk issue by ensuring HTTP traffic is securely redirected to HTTPS and to consider upgrading to TLS 1.3 for enhanced security.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The analysis identified that port **80** is open and associated with the HTTP service without encryption. This poses a risk if not redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled. The lack of encryption on this port could lead to interception of sensitive data, compromising business confidentiality.

Affected Assets:

- **IP Address: 66.22.23.14** - **Ports: 80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

It is recommended to configure the server to redirect all HTTP traffic on port **80** to HTTPS on port **443**. Additionally, enabling HSTS will ensure that browsers only connect over HTTPS, further securing data transmission.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The assessment revealed that the endpoint supports TLS 1.2, which is currently acceptable but does not support TLS 1.3, the current best practice for security and performance. The absence of TLS 1.3 could potentially impact data integrity and security.

Affected Assets:

- **Endpoint using TLS 1.2: 1**

Recommendations:

Upgrade the server configuration to support TLS 1.3 to enhance security and performance.

This will ensure compliance with modern cryptographic standards and provide better protection against potential vulnerabilities associated with older protocols.

1.4 General Recommendation

To enhance the overall security posture, it is crucial to address the Medium-risk issue by implementing HTTPS redirection and enabling HSTS for all HTTP traffic. Furthermore, upgrading to TLS 1.3 should be prioritized to align with current best practices in cryptographic security. Regular security assessments should be conducted to ensure ongoing protection against emerging threats and vulnerabilities.