1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings of a security assessment conducted on the domain **apps.topcoder.com**. The assessment was initiated on **April 4th** at **09:45** and completed in **00h:09m:32s**. The analysis was performed using a Basic scan methodology. The objective was to identify potential security vulnerabilities within the web application and its infrastructure, focusing on high and medium-risk issues.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** High, **1** Medium, **2** Low, and **15** informational. The most significant finding is a Medium-risk issue related to open port **80**, which lacks encryption and could expose data to interception if not redirected to HTTPS. This vulnerability requires immediate attention to ensure data integrity and confidentiality. Additionally, the SSL/TLS analysis revealed that all endpoints use TLS **1.2**, with no support for the more secure TLS **1.3**, indicating a potential area for improvement. The assessment also confirmed that no shared hosting environments or brute-force susceptible services were detected, reflecting a generally secure infrastructure. It is recommended to prioritize addressing the Medium-risk issue and consider upgrading to TLS **1.3** to enhance security posture.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security	Low
Login Form Detection Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description

The analysis identified that port **80** is open and running HTTP without encryption on IP address **52.3.25.55**. This poses a risk as data transmitted over HTTP can be intercepted by attackers, compromising data integrity and confidentiality.

Affected Assets

- IP Address: **52.3.25.55**
- Ports: **80/tcp** and **443/tcp**

Recommendations

Immediate action is required to configure a redirection from HTTP to HTTPS or enable HTTP Strict Transport Security (HSTS) to ensure that all communications are encrypted. This will mitigate the risk of data interception.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS analysis revealed that all endpoints are using TLS **1.2**, with no support for TLS **1.3**. While TLS **1.2** is currently acceptable, TLS **1.3** offers improved security and performance.

Affected Assets

- **3** endpoints using TLS **1.2**

Recommendations

It is recommended to upgrade the SSL/TLS configuration to support TLS **1.3**, enhancing the security posture by leveraging its advanced cryptographic algorithms and improved performance.

1.3.3 Login Form Detection Analysis

Description

The assessment detected **2** login forms within the application, which are considered Low risk but require validation to ensure secure authentication practices.

Affected Assets

- URLs:
  - `https://apps.topcoder.com/passwordless/start`
  - `http://apps.topcoder.com/passwordless/start`
  - `https://apps.topcoder.com/wiki/`

Recommendations

Conduct a thorough review of the login forms to ensure they implement secure authentication mechanisms, such as strong password policies and multi-factor authentication, to prevent unauthorized access.

1.4 General Recommendation

To enhance the overall security posture of the application, it is crucial to address the Medium-risk issue related to open port **80** by enforcing HTTPS across all endpoints. Additionally, upgrading to TLS **1.3** should be prioritized to leverage its enhanced security features. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.