# 1 Executive Security Assessment Report

## 1.1 Introduction

This security assessment was conducted on the domain `monster-customizer.classdojo.com` using a Basic analysis type. The scan was initiated on March 22 at 20:00 and completed in **00h:09m:15s**. The tracking ID for this assessment is **15e53117ab74**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

## 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 HTTP ports, which lack encryption and could expose sensitive data if not redirected to HTTPS. This vulnerability affects **25%** of the analyzed URLs, necessitating immediate review and potential implementation of HSTS. Additionally, the SSL/TLS protocols are well-configured, with all endpoints supporting TLS 1.2 and 1.3, ensuring robust encryption standards. The assessment also confirmed no shared hosting environments or high-density service configurations, indicating a secure infrastructure setup. It is recommended to address the HTTP port issue promptly to mitigate potential data exposure risks.

## 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 open HTTP ports that lack encryption, specifically port **80** associated with Amazon CloudFront httpd. This poses a risk as data transmitted over HTTP can be intercepted by attackers. Verification is needed to ensure redirection to HTTPS or enablement of HTTP Strict Transport Security (HSTS).

**Affected Assets**

- IP: **18.160.172.15**
- Ports: **80/tcp** and **443/tcp**

**Recommendations** Immediate action should be taken to configure the server to redirect HTTP traffic to HTTPS. Implementing HSTS will further enhance security by ensuring that browsers only connect over HTTPS.

### 1.3.2 SSL/TLS Protocols Security Assessment

**Description** The SSL/TLS configuration was found to be robust, with all endpoints supporting TLS 1.2 and TLS 1.3. No deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1 were detected, minimizing the risk of known cryptographic attacks.

**Affected Assets**

- **4** endpoints support TLS 1.3
- **4** endpoints use TLS 1.2

**Recommendations** Continue monitoring for updates in cryptographic standards and ensure that all systems are configured to support only secure protocols like TLS 1.2 and TLS 1.3.

### 1.3.3 Login Form Detection Analysis

**Description** A single login form was detected across the application, indicating a low risk level. However, it is essential to ensure that all authentication interfaces are secure against common attacks such as brute force or credential stuffing.

**Affected Assets**

- URLs:
  - `http://monster-customizer.classdojo.com:80`
  - `https://monster-customizer.classdojo.com:443`

**Recommendations** Implement security measures such as rate limiting, CAPTCHA, and multi-factor authentication (MFA) to protect login forms from unauthorized access attempts.

## 1.4 General Recommendation

It is crucial to address the Medium-risk issues related to open HTTP ports by enforcing HTTPS and implementing HSTS across all web services. Regularly update and review security configurations to align with best practices and emerging threats. Continuous monitoring and periodic security assessments are recommended to maintain a robust security posture.