# 1 Executive Security Assessment Report

## 1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **mtn-global.net**. The analysis was initiated on **June 13th** at **14:45** and completed in **14 minutes and 31 seconds**. The assessment was classified as a “Basic” type scan. The scope of the work included evaluating the security posture of the web application and its infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

## 1.2 Summary of Key Findings

The security assessment identified a total of **19 issues**, categorized as **1 High-risk**, **3 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical finding is the High-risk shared hosting environment, with one host sharing its IP with over **12,810 domains**, posing significant security risks. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, increasing vulnerability to cyber-attacks, and an SSL certificate nearing expiration in **66 days**, necessitating prompt renewal. Additionally, an Nmap scan revealed open HTTP ports without encryption, which should be addressed to prevent data breaches. Immediate actions include implementing a WAF, renewing SSL certificates, and securing open ports to mitigate potential threats.

## 1.3 Key Security Issues

| Title | Risk |
|---|---|
| Shared Hosting Environment Analysis | High |
| Absence of WAF | Medium |
| Nmap Port Scan Results Analysis | Medium |
| SSL Certificate Expiration Analysis | Medium |
| SSL/TLS Protocols Security Assess. | Low |

### 1.3.1 Shared Hosting Environment Analysis

**Description:**
The analysis identified a High-risk shared hosting environment where the host **mtn-global.net** shares its IP address with over **12,810 domains**. This configuration poses significant security risks due to shared infrastructure, increasing the likelihood of cross-contamination between domains.

**Affected Assets:**
- Hostname: **mtn-global.net**

**Recommendations:**
It is recommended to migrate to a dedicated hosting environment to isolate the domain from other potentially vulnerable domains. This will reduce the risk of cross-site contamination and improve overall security posture.

### 1.3.2 Absence of WAF

**Description:**
The absence of a Web Application Firewall (WAF) was noted on the analyzed host, resulting in a **100% vulnerability rate**. This significantly elevates the risk of successful cyber-attacks, particularly those involving injection-based attacks.

**Affected Assets:**
- Hostname: **mtn-global.net**

**Recommendations:**
Implement a robust WAF solution to protect against common web application attacks such as SQL injection, cross-site scripting (XSS), and other OWASP Top Ten vulnerabilities. Regularly update and configure the WAF rules to adapt to emerging threats.

### 1.3.3 Nmap Port Scan Results Analysis

**Description:**
The Nmap scan revealed that port **80/tcp** is open and running HTTP without encryption on IP **178.79.178.218**, posing a risk unless there is a redirection to HTTPS or HSTS is enabled.

**Affected Assets:**
- IP: **178.79.178.218** - Ports: **80/tcp**, **443/tcp** - Services: HTTP, SSL/HTTP - Version: nginx

**Recommendations:**
Ensure that all HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly monitor and update server configurations to maintain secure communication channels.

### 1.3.4 SSL Certificate Expiration Analysis

**Description:**
The SSL certificate for the domain **mtn-global.net** is set to expire in **66 days**, placing it in a warning status. Timely renewal is crucial to maintain secure communications.

**Affected Assets:**
- Domain: **mtn-global.net**

**Recommendations:**
Plan for the renewal of the SSL certificate well before its expiration date to avoid service disruptions and maintain trust with users. Consider implementing automated certificate management solutions to streamline the renewal process.

## 1.4 General Recommendations

To enhance the security posture of the domain **mtn-global.net**, it is recommended to address the identified vulnerabilities promptly. Implementing a dedicated hosting environment, deploying a Web Application Firewall (WAF), securing open ports, and ensuring timely SSL certificate renewals are critical steps in mitigating potential threats. Regular security assessments and continuous monitoring should be conducted to adapt to evolving cybersecurity challenges and maintain robust defenses against potential attacks.