1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **wirtgen-group-auf-der-bauma.com**. The assessment was initiated on **July 27th** at **03:45** and completed in **23 minutes and 9 seconds**. The analysis was performed using a Basic scan type. The scope of the work included evaluating the web application and its associated infrastructure for vulnerabilities, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **1** High-risk, **2** Medium-risk, **2** Low-risk, and **13** informational. The most critical finding is the High-risk shared hosting environment, where one host shares its IP with over **100** domains, potentially increasing exposure to cross-domain vulnerabilities. Medium-risk issues include insecure HTTP port exposure and an SSL certificate nearing expiration in **74** days, necessitating prompt renewal to maintain secure communications. The assessment also revealed that **100%** of servers are located in the Netherlands, with no High-risk geographic locations detected. While no immediate brute-force vulnerabilities were found, continuous monitoring and timely SSL renewals are recommended to mitigate potential risks.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description:
The domain **wirtgen-group-auf-der-bauma.com** is hosted in a shared environment with over **163** domains on the same IP address. This configuration poses a High risk due to potential cross-domain vulnerabilities that can arise from shared infrastructure.

Affected Assets:
- Hostname: **wirtgen-group-auf-der-bauma.com**

Recommendations:
It is recommended to migrate to a dedicated hosting environment to minimize exposure to cross-domain vulnerabilities. Implementing strict access controls and monitoring for unusual activities can further enhance security.

1.4.2 Nmap Port Scan Results Analysis

Description:
An open HTTP port (**80/tcp**) was detected on IP **13.81.242.183**, running Apache httpd without encryption. This poses a Medium risk as it may allow unencrypted data transmission.

Affected Assets:
- IP: **13.81.242.183** - Ports: **80/tcp**, **443/tcp**

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly update server software to mitigate known vulnerabilities.

1.4.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **wirtgen-group-auf-der-bauma.com** is set to expire in **74** days, categorized under the “Warning” risk level, indicating that renewal planning should occur soon.

Affected Assets:
- Domain: **wirtgen-group-auf-der-bauma.com**

Recommendations:
Plan for the renewal of the SSL certificate well before the expiration date to ensure uninterrupted secure communications. Consider automating certificate management to avoid future lapses.

1.5 General Recommendations

To enhance overall security posture, it is advised to implement continuous monitoring and regular security assessments. Ensure all software components are up-to-date and apply security patches promptly. Additionally, consider adopting advanced security measures such as intrusion detection systems (IDS) and web application firewalls (WAF) to protect against emerging threats.