1 Executive Security Assessment Report

1.1 Overview

The security assessment was conducted on the domain **part-info-cons.services.wirtgen-group.com**. The analysis was initiated on **04-08** at **20:00** and completed in **00h:05m:32s**. The assessment type was classified as **Basic**. The scope of the work included a comprehensive evaluation of the domain's security posture, focusing on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Summary of Findings

The recent security assessment revealed no High, Medium, or Low-risk issues, with **three** informational findings. Notably, all scanned ports (**11** in total) were filtered, indicating robust perimeter security controls such as firewalls and IPS/IDS systems. The analysis confirmed no shared hosting environments, with all hosts on dedicated infrastructure, mitigating potential shared hosting risks. Additionally, the geographic distribution analysis showed all servers located in Germany, with no presence in high-risk locations, ensuring a normal risk status. These findings underscore the effectiveness of current security measures, though manual verification is advised to confirm automated assessment results.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues Identified	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk vulnerabilities. This indicates a strong security posture for the domain **part-info-cons.services.wirtgen-group.com**. The absence of critical vulnerabilities suggests that existing security controls are effective in mitigating potential threats.

1.4.2 Affected Assets

- Domain: **part-info-cons.services.wirtgen-group.com**

1.4.3 Recommendations

While no High or Medium-risk issues were identified, it is recommended to continue regular security assessments to maintain the current security posture. Additionally, consider conducting manual verification to ensure the accuracy of automated findings. Regular updates and patches should be applied to all systems to protect against emerging threats. Implementing a continuous monitoring strategy will help in promptly identifying and addressing any future vulnerabilities.

1.5 General Recommendation

To maintain and enhance the current security posture, it is advisable to implement a robust security management program that includes regular vulnerability assessments, patch management, and continuous monitoring. Engaging in periodic security training for staff and ensuring compliance with industry standards will further strengthen the organization's defense mechanisms against potential cyber threats.