1 Executive Security Assessment Report

1.1 Overview

The security assessment was conducted on the domain **wirexchangeservices-qa.goxroads.com**. The analysis commenced on **March 30th** at **10:45** and concluded in **00h:11m:27s**. The assessment was identified with tracking ID **03021e538cc5** and was performed as a **Basic** type scan. The evaluation focused on identifying high and medium-risk vulnerabilities within the domain's infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **0** high-risk, **1** medium-risk, **1** low-risk, and **16** informational. The most significant finding is the medium-risk issue related to subdomain naming, which could expose sensitive endpoints and increase the risk of unauthorized access to critical systems. Additionally, the low-risk SSL/TLS protocol assessment indicates the use of TLS 1.2, with no support for the more secure TLS 1.3, suggesting a need for protocol upgrades to enhance security. The analysis also confirmed no shared hosting environments, normal geographic distribution, and no unusual port assignments, indicating a generally secure infrastructure. It is recommended to address the subdomain naming vulnerabilities and consider upgrading to TLS 1.3 to mitigate potential risks.

1.3 Key Security Issues

Title	Risk
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Subdomain Naming Security Assessment

Description

The assessment identified a medium-risk issue concerning subdomain naming conventions. A total of **1** sensitive subdomain was detected, which could potentially provide unauthorized access to administrative interfaces, internal systems, or development environments. These endpoints may expose critical systems and sensitive data, increasing the risk of exploitation.

Affected Assets

- Subdomain: **wirexchangeservices-qa.goxroads.com**

Recommendations

It is recommended to review and modify subdomain naming conventions to avoid disclosing sensitive information about the infrastructure. Implement access controls and monitoring on sensitive subdomains to detect and prevent unauthorized access. Regular audits should be conducted to ensure compliance with best practices for subdomain management.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS protocol assessment revealed that the domain supports TLS 1.2 but lacks support for TLS 1.3, which is considered the current best practice for enhanced security and performance. While TLS 1.2 is acceptable, upgrading to TLS 1.3 would provide improved cryptographic strength and performance benefits.

Affected Assets

- **1** endpoint using TLS 1.2
- No endpoints using TLS 1.3

Recommendations

It is advised to upgrade the SSL/TLS configuration to support TLS 1.3 across all endpoints to align with modern security standards. This upgrade will enhance the cryptographic security of data in transit and improve overall system performance.

1.4 General Recommendations

To strengthen the security posture of the domain **wirexchangeservices-qa.goxroads.com**, it is crucial to address the identified medium-risk issue related to subdomain naming and consider upgrading the SSL/TLS protocols to include TLS 1.3 support. Regular security audits and adherence to best practices will help maintain a robust defense against potential threats.