1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **wsvepts-test.polcard.com.pl**. The analysis was initiated on **July 20th** at **06:00** and completed in **21 minutes and 49 seconds**. The assessment type was classified as **Basic**. The evaluation focused on identifying vulnerabilities within the web application and infrastructure, employing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Findings

The security assessment identified a total of **19 issues**, categorized as **1 high-risk**, **1 medium-risk**, **3 low-risk**, and **14 informational**. The most critical finding is a high-risk Denial of Service (DoS) vulnerability on port **80**, with a **97.76% timeout rate**, posing a significant threat to service availability. A medium-risk issue involves potentially sensitive subdomains, which could expose critical systems to unauthorized access.

1.3 Issues Table

Title	Risk
Denial of Service (DoS) Vulnerability	High
Subdomain Naming Security Assessment	Medium
API Surface Analysis	Low
TCP-Wrapped Ports - Possible Firewall/Security Controls	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Denial of Service (DoS) Vulnerability Assessment

Description:
A high-risk Denial of Service (DoS) vulnerability was identified on port **80** of the domain wsvepts-test.polcard.com.pl. The analysis revealed a **97.76% timeout rate** for HTTP requests, indicating a severe risk to service availability. Port **443** showed no timeouts, suggesting a lower risk for HTTPS services.

Affected Assets:
- Endpoint: **wsvepts-test.polcard.com.pl:80**

Recommendations:
- Immediate review and adjustment of firewall rules to limit excessive connections. - Implement specific DoS protection mechanisms for the affected endpoint. - Monitor server performance closely during peak traffic periods. - Optimize server response configurations to mitigate potential DoS attacks.

1.4.2 Subdomain Naming Security Assessment

Description:
The assessment identified a medium-risk issue involving potentially sensitive subdomains. A total of **1 sensitive subdomain** was detected, indicating possible exposure of administrative interfaces or development environments.

Affected Assets:
- Subdomain: **wsvepts-test.polcard.com.pl**

Recommendations:
- Conduct thorough security reviews of all identified subdomains. - Restrict access to sensitive subdomains using authentication and IP whitelisting. - Regularly audit subdomain configurations to ensure they do not expose critical systems.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the remediation of high-risk vulnerabilities immediately. Continuous monitoring and regular security assessments should be conducted to identify and mitigate medium and low-risk issues. Implementing robust access controls, maintaining updated security patches, and conducting employee training on security best practices are essential steps in safeguarding the organization's digital assets.