1 Executive Security Assessment Report

1.1 Introduction

This report provides an executive summary of the security assessment conducted on the domain **sbizbillpay-test.zionsbank.com**. The analysis was performed using a certified and qualified web application and infrastructure penetration testing tool, adhering to OWASP and OSCP methodologies. The assessment commenced on **May 29th at 09:00** and concluded in **00h:10m:40s**. The tracking ID for this assessment is **0443285e925b**, and the scope included a basic evaluation of the domain's security posture.

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 a medium-risk issue related to subdomain naming, which could expose sensitive endpoints and increase the risk of unauthorized access to development or staging environments. Additionally, the low-risk issue pertains to SSL/TLS protocols, with only TLS 1.2 in use and no support for the more secure TLS 1.3, potentially impacting data transmission security. Notably, **100%** of servers are located in the United States, with no high-risk geographic locations detected. The assessment also confirmed no unusual port assignments or brute-force vulnerable services, indicating a generally secure infrastructure. Immediate attention should focus on securing sensitive subdomains and upgrading to TLS 1.3 to enhance security posture.

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 the naming of subdomains. Specifically, the subdomain **sbizbillpay-test.zionsbank.com** was detected, indicating a development or staging environment. Such environments may contain unpatched vulnerabilities or debug information that could be exploited by unauthorized users. These environments often provide access to critical systems and sensitive data, including administrative and monitoring interfaces that might expose internal system details.

Affected Assets

- Subdomain: **sbizbillpay-test.zionsbank.com**

Recommendations

To mitigate this risk, it is recommended to implement strict access controls on development and staging environments. Consider using VPNs or IP whitelisting to restrict access. Regularly audit these environments for vulnerabilities and ensure that they are not publicly accessible unless absolutely necessary. Additionally, consider renaming subdomains to non-descriptive names that do not reveal their purpose.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS protocol assessment revealed a low-risk issue due to the exclusive use of TLS 1.2 across all endpoints, with no support for the more secure TLS 1.3 protocol. While TLS 1.2 is currently acceptable, TLS 1.3 offers enhanced security features and improved performance, which are critical for protecting data transmission against potential threats.

Affected Assets

- **1 endpoint** using TLS 1.2

Recommendations

It is recommended to upgrade all endpoints to support TLS 1.3 to align with current best practices for security and performance. This upgrade will provide improved cryptographic algorithms and reduce the risk of vulnerabilities associated with older protocols. Ensure that all systems are configured to prioritize TLS 1.3 connections where possible.

1.4 General Recommendation

Overall, the security posture of the domain is robust, with no high-risk issues detected. However, attention should be directed towards addressing the medium-risk subdomain naming issue and upgrading SSL/TLS protocols to enhance security measures further. Regular security audits and adherence to best practices will help maintain a secure environment and protect against emerging threats.