



Web Application Penetration Testing Report (updated)

FortVault LLC.

June 2026

Business Risk Services



Contents

Web Application Penetration Testing Report (updated)	1
Background	2
Scope	2
Approach	3
Field Work	3
General conclusion	3
Acknowledgment	4
Key Findings	4
Risk Rating	4

Executive Summary

Background

In accordance with the contract [REDACTED] signed between the FortVault LLC (Furthermore the Client) and Grant Thornton Consulting CJSC, we have performed a web application penetration testing.

In recent years there has been marked increase of security events and hacking attempts in all industries, especially where large amounts of sensitive data such as payment cards or client information are being stored. The consequences of an attack could be varied, with the systems possibly corrupted, unavailable, and out of action with all the consequent risks of data loss, financial loss and reputational issues.

New vulnerabilities are reported every day making it virtually impossible for IT teams to keep up to date. An effective network security control environment and secure applications is therefore fundamental in ensuring the integrity of information and the on-going protection of IT assets.

The purpose of the penetration testing was to conduct an independent assessment over the adequacy and integrity of the tested web application at the time of our penetration testing, against known exploits, vulnerabilities, and misconfigurations.

Scope

Penetration testing was performed from Grant Thornton premises and cloud-based attack platform via internet connection. The FortVault LLC representatives provided us some information to start assessment. Scope was defined as the following web applications, which described in Table 1.

A test account was provided by the Client, as detailed in Table 2. Any additional testing was conducted using publicly accessible functionality and accounts created by the assessment team.

Table 1: In Scope components

URL	Comment
[REDACTED]	[REDACTED]

Table 2: Accounts used

[REDACTED]
[REDACTED]
[REDACTED]

Approach

The objective of the penetration testing was to assess the effectiveness of information security controls for external threats and their ability to protect access to confidential information. The penetration testing has used a combination of attacks and penetration techniques and technology exploits to obtain access to the client's data from external facing networks.

The penetration testing was conducted using user credentials provided by the Client. All testing activities were performed in a white box environment.

The engagement included two stages: the initial web application penetration testing and a follow-up remediation validation review. During the initial testing phase, Grant Thornton identified and documented the exposed [REDACTED] vulnerability in the original report delivered to the Client. After the Client implemented remediation measures, Grant Thornton performed validation procedures to determine whether the previously identified issue remained present in the tested environment.

Field Work

Web Application Penetration Testing

We attempted to gain information and exploit “██████████” application by using all publicly available resources.

General conclusion

Experience has shown that a focused effort to address the weaknesses outlined in this report can result in security improvements. Most of identified weaknesses do not require high-tech solutions, just knowledge of and commitment to good practices.

For the systems to remain secure, however, security posture should be evaluated and improved continuously. Establishing the organizational structure that will support these ongoing improvements is essential to maintain control of corporate information systems.

During the initial assessment, Grant Thornton identified one Medium-rated vulnerability related to exposed ██████████. The issue was documented in the original report delivered to the Client. Following report delivery, the Client implemented remediation measures, and Grant Thornton’s follow-up validation confirmed that the vulnerability was no longer observed in the tested environment. Based on the validation results, the finding is considered Remediated.

Acknowledgment

We would like to take this opportunity to thank the FortVault LLC management and staff for their cooperation during this assignment.

Key Findings

Area/Risk	Critical	High	Medium	Low
Web application Assessment	-	-	-	-

Risk Rating

Risk rating based on the updated penetration testing results for FortVault LLC Web Application is considered Low. ██████████ identified during the initial assessment. However, the Client remediated ██████ after the initial report delivery. During follow-up validation, Grant Thornton did not observe the previously identified vulnerability in the tested environment.

Additionally, the assessment did not identify a direct path from an external attacker to full system compromise. Grant Thornton recommends that FortVault LLC continue periodic security testing, secure configuration reviews, and patch management to preserve the improved security posture.

