June 13, 2025

Prepared for Very Good Security

Web Application Penetration Test

Project
Ethical Hacking Report Deliverable

Version
1.0

Table of Contents

1.0 Executive Summary

NetWorks Group (NWG) completed an in-depth Web Application Penetration Test for Very Good Security (VGS) on June 13, 2025. The objective of this test was to assess the security of VGS's Dashboard web application and associated APIs. NWG utilizes the standards set by the Open Web Application Security Project (OWASP) Web Security Testing Framework as a baseline for testing. This report includes the results of testing domains as outlined by OWASP as well as any additional findings, and provides recommendations as they relate to best practices and compliance.

This report's results and recommendations are intended to help VGS make informed decisions about its security and implement best practices and compliance measures to better defend against potential threats. By taking a proactive approach to security, organizations like VGS can reduce the risk of a breach and protect their valuable assets.

POSITIVE EFFORTS

- All data-in-transit for sites in scope is protected by TLS 1.2 or higher by default. Attempts to negotiate a less secure connection were refused.
- No rogue directories or files were identified during the penetration test.
- A well-formatted Content Security Policy header is in place.
- A strong password policy is implemented, with a 12-character minimum and complexity requirements.
- Password reset links are one-time use and expire if not used after a reasonable period of time.
- Robust server-side data sanitization thwarted all attempted injection attacks.
- All attempted path/directory traversal attacks were unsuccessful.
- All identified Amazon S3 buckets were protected.
- Attempted authentication bypass attacks failed - requests to make, modify, or delete data without the proper authentication token or session cookie failed.
- Short idle-session timeouts are in place.
- Attempted open redirect attacks were unsuccessful.
- Attempts to inject API calls with malicious or unexpected inputs did not result in information disclosure or unhandled exceptions.

1.1 Risk Score

The following score represents NWG's best estimate of risk in VGS's Dashboard web application. Risk is calculated based on the severity of individual findings in each testing domain. Risk score criteria are detailed further in **Appendix B**.

Dashboard	**LOW RISK**

1.2 Findings Summary

The table below summarizes the results of testing for each of the 2021 OWASP Top 10 vulnerabilities for web applications.

OWASP Top 10	RISK	FINDINGS
A01 Broken Access Control	*N/A*	*None*
A02 Cryptographic Failures	*N/A*	*None*
A03 Injection	*N/A*	*None*
A04 Insecure Design	*N/A*	*None*
A05 Security Misconfiguration	*N/A*	*None*
A06 Vulnerable and Outdated Components	**Low**	**Vulnerable JavaScript Dependencies**
A07 Identification and Authentication Failures	*N/A*	*None*
A08 Software and Data Integrity Failures	*N/A*	*None*
A09 Security Logging and Monitoring Failures	*N/A*	*None*
A10 Server-Side Request Forgery	*N/A*	*None*
Other Testing	*N/A*	*None*

2.0 Testing Methodology

NWG follows a standardized and structured approach while conducting web application penetration tests that sorts attack vectors into twelve distinct testing domains. NWG simulates the current threat landscape by utilizing both automated and manual tools that are illustrative of the tactics used by threat actors to test the security of web applications in each domain.

NWG Web Application Penetration Testing Domains	
INFORMATION GATHERING	NWG employs passive and active reconnaissance on both publicly available and obfuscated data that can be accessed without exploitation of vulnerabilities.
CONFIGURATION AND DEPLOYMENT MANAGEMENT	NWG searches for insecure default configurations, the inadvertent inclusion of development tools, or any other weakness which could disclose critical information about the system's architecture.
IDENTITY MANAGEMENT	NWG examines user roles, registration, provisioning, and account username policies within the application that could facilitate impersonation of another account.
AUTHENTICATION	NWG attempts to bypass or manipulate controls to compromise user credentials.
AUTHORIZATION	NWG tests for weakness that permit users to perform actions beyond their intended scope.
SESSION MANAGEMENT	NWG searches for weaknesses that could lead to session hijacking, fixation, or other compromises of user sessions.
INPUT VALIDATION	NWG employs techniques and tradecraft to identify ineffective input validation and demonstrates potential impact with proof-of-concept attacks.
ERROR HANDLING	NWG probes for instances where error messages divulge sensitive information, such as database schema, file paths, or other internal system details which could aid threat actors.
CRYPTOGRAPHY	NWG evaluates key management practices and overall encryption implementation.
BUSINESS LOGIC	NWG analyzes workflows, rules, and processes to identify potential weaknesses in the application's design.
CLIENT-SIDE	NWG attempts to inject scripts, manipulate local storage, or otherwise tamper with client-side processes and data.
API	NWG assesses relevant API's functionalities, security measures, and access controls.
OTHER	NWG examines the technologies in use by the application and its unique functions to determine if any other findings not included in the twelve testing domains are relevant.

3.0 Matters Requiring Attention

This section details specific problems that may increase the likelihood of a successful compromise. These items are often security best practices that the tester has directly observed, facilitated some compromise, or combined. These are consultative measures and are prioritized remediation guidelines to direct overall security strategy when reviewing this report. A detailed explanation of NWG scoring can be found in **Appendix B**. NWG has identified the following Matters Requiring Attention (MRAs).

3.1 Vulnerable JavaScript Dependencies	
URL	**Axios 0.21.4** • https://js.verygoodvault.com/vgs-collect/2.18.6/vgs-collect.js **Axios 1.7.9** • https://www.verygoodsecurity.com/docs/app-39b4d099680626c209e8.js
Severity	**Low**
Finding	NWG Penetration testers identified two instances of vulnerable JavaScript dependencies (OWASP Top 10 A06 Vulnerable and Outdated Components) in use for the sites in scope: **Axios 0.21.4**, which contains the following vulnerabilities: • CVE-2023-45857, An issue discovered in Axios 1.5.1 inadvertently reveals the confidential XSRF-TOKEN stored in cookies by including it in the HTTP header X-XSRF-TOKEN for every request made to any host allowing attackers to view sensitive information. • CVE-2025-27152, axios is a promise-based HTTP client for the browser and node.js. The issue occurs when passing absolute URLs rather than protocol-relative URLs to axios. Even if baseURL is set, Axios sends the request to the specified absolute URL, potentially causing SSRF and credential leakage. This issue impacts both server-side and client-side usage of Axios. This issue is fixed in 1.8.2. and **Axios 1.7.9**, which contains the following vulnerabilities: • CVE-2025-27152 (see above).

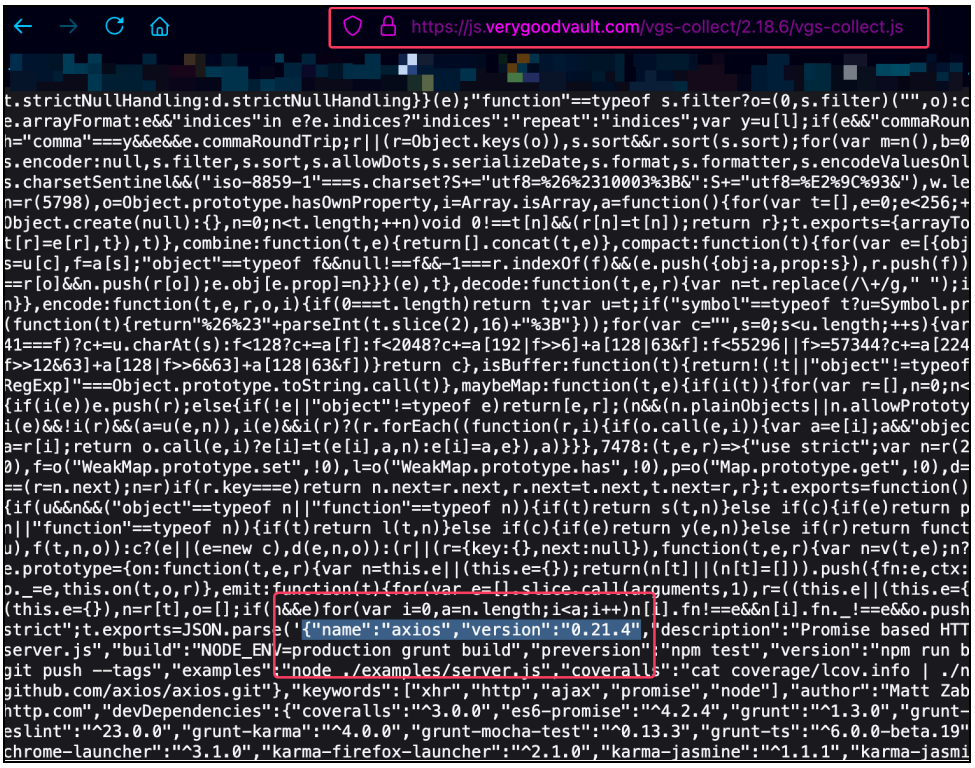

Figure 1. Axios v0.21.4 in use in verygoodvault

During the penetration test, we were unsuccessful in our efforts to exploit the underlying CVEs in order to elevate our privilege or achieve server-side request forgeries (SSRFs).

Recommendations	Reduce attack surface by continuously removing unused features, components, files, and documentation. Leverage tools like Dependabot to continuously monitor for vulnerable and outdated components in the existing code base. Continuously update dependencies to the latest supported version.
References	• https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ • https://cwe.mitre.org/data/definitions/1035.html • https://nvd.nist.gov/vuln/detail/CVE-2023-45857 • https://nvd.nist.gov/vuln/detail/CVE-2025-27152

4.0 Roadmap

The Remediation Roadmap provides VGS with NWG's best estimate of an appropriate timeline for remediating the findings detailed in this report. The suggested timeline is based on NWG's years of observations, the urgency of the issue, and the time it will realistically take to implement. Also included are suggestions for other security testing activities based on industry standards for frequency.

IMMEDIATE	Develop a plan to prioritize and remediate findings. Remove any accounts created for testing.
SHORT TERM	Continue practicing secure coding techniques and development.
LONG TERM	Create or review incident response plan. Identify and remediate applications performing external interactions.
ANNUAL	Conduct web application assessments annually or whenever significant changes are implemented.

Appendix A Scope

Testing Began	June 09, 2025
Testing Completed	June 13, 2025
Additional Credentials Provided	Yes
Web Application URL(s)	• https://dashboard.verygoodsecurity.com • https://api.live.verygoodsecurity.com/ • https://api.sandbox.verygoodsecurity.com/ • https://tnt2vligzvq.sandbox.verygoodproxy.com • https://tnt2vligzvq-4fea4709-65d0-4607-9e0e-8ef5e452f834.sandbox.verygoodproxy.com/post

Appendix B Definitions

Risk ratings and severity scores presented throughout this document are determined based on NWG's years of experience in conducting security assessments. The following definitions categorize how NWG determines the scores issued:

Risk Scores

Risk ratings presented in **Section 1.1 Risk Score** are the cumulative representation of the severity of findings discovered.

Severity Scores

Severity scores of "critical", "high", "medium", "low", and "informational" are issued in **Section 3.0 Matters Requiring Attention**. These scores are based on NWG's years of experience in conducting security assessments.

Critical	A "critical" severity finding represents a significant, imminent threat to the organization or would have egregious consequences if leveraged by an attacker. Critical vulnerabilities should be addressed immediately.
High	A "high" severity finding represents a likely threat to the organization. These vulnerabilities should be addressed as soon as possible.
Medium	A "medium" severity finding poses some threat to the organization or its data or may be utilized in conjunction with other vulnerabilities in order to compromise the organization further.
Low	A "low" severity finding may give an attacker useful information about the organization or aid in additional attacks.
Informational	An "informational" finding, while not posing a specific threat, denotes relevant observations made during the engagement that were not categorized as vulnerabilities.