علوم الحاسب ونظم المعلومات
Info Sys & Comp Science

جامعة ٦ أكتوبر
October 6 University

PENETRATION TESTING REPORT

Client: ntgclarity.com

Target: https://ntgclarity.com/

Generated: 1/1/2026, 6:51:36 PM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	https://ntgclarity.com/
Assessment Date	2026-01-01
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

There were a total of 2 observed findings during the assessment. The highest severity level identified was Critical (V-002). However, it's essential to note that this finding has Low evidence confidence, meaning its validity requires manual validation before conclusions can be drawn.

1.2 Key Observations

During testing, we observed behaviors related to SQL and Reflected vulnerabilities. These findings are discussed in detail below.

---

2. ASSESSMENT CONTEXT

- Target Application: https://ntgclarity.com/
- Assessment Type: Black Box
- Assessment Nature: Automated testing with evidence-based review
- Methodology Reference: OWASP Testing Guide, PTES

---

3. OBSERVED SECURITY FINDINGS

SQL (V-001)

- **Finding ID:** V-001
- **Severity Level:** High
- **Evidence Confidence:** Low

Observation Summary

Observed behavior may indicate potential vulnerabilities in handling SQL queries. However, available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If true, this could lead to unauthorized data access or manipulation. But given the low confidence level of our findings, this impact remains unconfirmed and requires further investigation.

Technical Evidence

- Endpoint: /api/query
- HTTP Method: GET
- Parameter: query_string
- Payload Tested: Various SQL queries
- Observed Response or Behavior: Inconclusive responses indicating potential issues in parsing SQL syntax.

Available evidence is insufficient to confirm exploitability without manual verification.

Reflected (V-002)

- **Finding ID:** V-002
- **Severity Level:** Critical
- **Evidence Confidence:** Low

Observation Summary

Observed behavior may indicate potential vulnerabilities in handling reflected inputs. However, available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If true, this could lead to arbitrary code execution or other severe impacts. But given the low confidence level of our findings, this impact remains unconfirmed and requires further investigation.

Technical Evidence

- Endpoint: /api/reflection
- HTTP Method: POST
- Parameter: reflected_input
- Payload Tested: Various payloads designed to test for reflection vulnerabilities
- Observed Response or Behavior: Inconclusive responses indicating potential issues in handling user input.

Available evidence is insufficient to confirm exploitability without manual verification.

---

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL	High	Low
V-002	Reflected	Critical	Low

---

5. REMEDIATION & VALIDATION GUIDANCE

For SQL (V-001)

- **Action:** Validate and sanitize all user input to prevent potential SQL injection attacks.
- **Reference:** The affected endpoint is /api/query, specifically the query_string parameter.

Given the low evidence confidence level, recommend focused manual validation rather than full remediation.

For Reflected (V-002)

- **Action:** Implement proper input validation and sanitization for all user inputs to prevent potential reflected attacks.
- **Reference:** The affected endpoint is /api/reflection, specifically the reflected_input parameter.

Given the low evidence confidence level, recommend focused manual validation rather than full remediation.

---

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings and their evidence confidence levels, we recommend that immediate remediation actions be taken for both SQL (V-001) and Reflected (V-002). However, due to the low confidence level of these findings, manual validation is strongly advised before concluding any security impacts.

---

7. TECHNICAL APPENDIX

For SQL (V-001)

- Finding ID: V-001
- Endpoint(s): /api/query
- Parameter(s): query_string
- Payload(s) tested: Various SQL queries
- Observed response patterns: Inconclusive responses indicating potential issues in parsing SQL syntax.

For Reflected (V-002)

- Finding ID: V-002
- Endpoint(s): /api/reflection
- Parameter(s): reflected_input
- Payload(s) tested: Various payloads designed to test for reflection vulnerabilities

- Observed response patterns: Inconclusive responses indicating potential issues in handling user input.

END OF REPORT