علوم الحاسب ونظم المعلومات
Info Sys & Comp Science

جامعة ٦ أكتوبر
October 6 University

🔒 PENETRATION TESTING REPORT

Client: testhtml5.vulnweb

Target: http://testhtml5.vulnweb.com

Generated: 1/1/2026, 9:26:55 PM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	http://testhtml5.vulnweb.com
Assessment Date	2026-01-01
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

Total number of observed findings: 6. Highest severity level identified: Medium. Overall confidence level of the available evidence is generally Low to Medium.

Some High and Critical severity findings exist with Low or Medium evidence confidence, requiring manual validation before conclusions can be drawn.

1.2 Key Observations

Observed behaviors include potential information disclosure headers, missing security headers, behavioral anomalies during testing, and time-based delays in responses.

---

2. ASSESSMENT CONTEXT

- Target Application: http://testhtml5.vulnweb.com
- Assessment Type: Black Box
- Assessment Nature: Automated testing with evidence-based review
- Methodology Reference: OWASP Testing Guide, PTES

---

3. OBSERVED SECURITY FINDINGS

V-001 - Behavioral Anomaly Observed During Testing

- **Finding ID:** V-001
- **Severity Level:** Medium
- **Evidence Confidence:** Medium

Observation Summary

Observed behavioral anomalies during testing at the affected endpoint, potentially indicating a security issue.

Why This Matters

The observed behavior may indicate an information disclosure or other security-related vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Behavioral anomaly observed during testing

V-002 - INFO DISCLOSURE HEADERS

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

Observation Summary

Observed potential information disclosure headers at the affected endpoint.

Why This Matters

The observed behavior may indicate an information disclosure vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Behavioral anomaly observed during testing

V-003 - MISSING SECURITY HEADERS

- **Finding ID:** V-003
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed missing security headers at the affected endpoint.

Why This Matters

The absence of these headers may indicate a potential vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Missing security headers

V-004 - PERMISSIONS POLICY

- **Finding ID:** V-004
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavioral anomalies during testing at the affected endpoint, potentially indicating a permissions policy issue.

Why This Matters

The observed behavior may indicate an information disclosure or other security-related vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Behavioral anomaly observed during testing

V-005 - POC RUNNER SCANNER

- **Finding ID:** V-005
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavioral anomalies during testing at the affected endpoint, potentially indicating a vulnerability related to a proof-of-concept runner scanner.

Why This Matters

The observed behavior may indicate an information disclosure or other security-related vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Behavioral anomaly observed during testing

V-006 - TLS SECURITY CHECK

- **Finding ID:** V-006
- **Severity Level:** Medium
- **Evidence Confidence:** Low

Observation Summary

Observed behavioral anomalies during testing at the affected endpoint, potentially indicating a vulnerability related to TLS security.

Why This Matters

The observed behavior may indicate an information disclosure or other security-related vulnerability. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: Not specified
- HTTP Method: GET
- Parameter: Not specified
- Payload Tested: Not captured
- Observed Response or Behavior: Behavioral anomaly observed during testing

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	Behavioral Anomaly Observed During Testing	Medium	Medium
V-002	INFO DISCLOSURE HEADERS	Medium	Low
V-003	MISSING SECURITY HEADERS	Medium	Low
V-004	PERMISSIONS POLICY	Medium	Low
V-005	POC RUNNER SCANNER	Medium	Low
V-006	TLS SECURITY CHECK	Medium	Low

5. REMEDIATION & VALIDATION GUIDANCE

V-001 - Behavioral Anomaly Observed During Testing

Recommend manual validation to confirm the existence and impact of this behavior.

V-002 - INFO DISCLOSURE HEADERS

Manually verify if these headers indeed disclose sensitive information. Adjust security headers accordingly based on findings.

V-003 - MISSING SECURITY HEADERS

Implement missing security headers (Content-Security-Policy, X-Frame-Options, etc.) to enhance the application's security posture.

V-004 - PERMISSIONS POLICY

Manually validate if permissions policies are correctly configured and enforced. Adjust access controls as necessary based on findings.

V-005 - POC RUNNER SCANNER

Verify if this scanner indeed poses a vulnerability. If so, implement appropriate mitigations to prevent exploitation.

V-006 - TLS SECURITY CHECK

Validate the security of your TLS configuration by implementing best practices (e.g., using secure ciphers and protocols).

6. OVERALL ASSESSMENT VERDICT

Based on observed findings with generally Low to Medium evidence confidence, recommend routine security hardening measures. Manual validation is required for High or Critical severity findings.

7. TECHNICAL APPENDIX

V-001 - Behavioral Anomaly Observed During Testing

- Finding ID: V-001
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Behavioral anomaly observed during testing

V-002 - INFO DISCLOSURE HEADERS

- Finding ID: V-002
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Behavioral anomaly observed during testing

V-003 - MISSING SECURITY HEADERS

- Finding ID: V-003
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Missing security headers

V-004 - PERMISSIONS POLICY

- Finding ID: V-004
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Behavioral anomaly observed during testing

V-005 - POC RUNNER SCANNER

- Finding ID: V-005
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Behavioral anomaly observed during testing

V-006 - TLS SECURITY CHECK

- Finding ID: V-006
- Endpoint(s): Not specified
- Parameter(s): Not specified
- Payload(s) tested: Not captured
- Observed response patterns: Behavioral anomaly observed during testing