CONFIDENTIAL — SAMPLE / DEMONSTRATION

WEB APPLICATION PENETRATION TESTING REPORT

2026 Illustrative Sample Deliverable

Organization	NorthStar Digital Commerce, Inc. (Fictional)
Application	NorthStar Commerce Portal (Fictional)
Prepared By	TMG Security
Assessment Type	Web Application Penetration Test
Assessment Period	01 August 2026 – 31 August 2026
Report Date	10 September 2026
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION

FICTIONAL SAMPLE REPORT

NOT AN ACTUAL CLIENT ASSESSMENT

All findings, evidence, and results are illustrative.

01 DOCUMENT CONTROL

Document Title	Web Application Penetration Testing Report — NorthStar Commerce Portal (Fictional Sample)
Document ID	TMG-WAPT-NDC-2026-001
Version	1.0
Issue Date	10 September 2026
Assessment Period	01 August 2026 – 31 August 2026
Assessment Type	Web Application Penetration Test
Client	NorthStar Digital Commerce, Inc. (Fictional)
Application	NorthStar Commerce Portal (Fictional) — https://portal.northstar-example.com (Fictional URL)
Environment	Fictional staging / controlled assessment environment
Prepared By	TMG Security Offensive Security Team
Technical Lead	TMG Security — Senior Penetration Tester (Fictional Engagement Role)
Reviewed By	TMG Security Quality Assurance Lead
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION

Version History

Version	Date	Author	Summary
1.0	10 September 2026	TMG Security Offensive Security Team	Initial issue — fictional sample deliverable.

02 IMPORTANT DISCLAIMER

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL CLIENT PENETRATION TEST

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, technical depth, and professional reporting standard of a web application penetration testing deliverable. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- NorthStar Digital Commerce, Inc. is a fictional entity. It does not correspond to any real company, and any resemblance to an actual organization is purely coincidental.
- NorthStar Commerce Portal is a fictional application. No real production system was built, deployed, or accessed.
- The application URL referenced throughout this report (https://portal.northstar-example.com) is a fictional, non-resolving placeholder domain used only for illustration.
- No real client was engaged and no real client environment was tested.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report.
- No real user data, personal information, or customer records were accessed, viewed, or processed.
- No real credentials — including cloud, application, or third-party credentials — were used or are disclosed anywhere in this report.
- All vulnerabilities, findings, risk ratings, dates, and remediation statuses described in this report are fictional and were constructed for demonstration purposes.
- All Proofs of Concept (PoCs) are illustrative, synthetic, and non-destructive; none were executed against a real or live target.
- All CVSS-style scores in this report are illustrative and do not reflect the scoring of any actual vulnerability.
- All screenshots, request/response examples, and evidence panels are synthetic or simulated representations created specifically for this sample report.
- No real exploitation occurred at any point during the preparation of this document, and no actual customer impact occurred.
- This report does not represent an actual TMG Security client engagement and must not be relied upon as evidence of the security posture of any real organization.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's offensive-security methodology, technical reporting standards, and evidence-presentation quality. It should not be relied upon for any compliance, legal, contractual, or procurement decision, and does not constitute security advice regarding any real system.

TABLE OF CONTENTS

03 EXECUTIVE SUMMARY

TMG Security has prepared this fictional, illustrative Web Application Penetration Testing report to represent NorthStar Digital Commerce, Inc., a hypothetical U.S.-based e-commerce / SaaS / digital-payments company, and its fictional flagship application, the NorthStar Commerce Portal. This section presents a fictional executive-level summary of the simulated assessment, prepared in the style and format TMG Security would use for an actual client engagement.

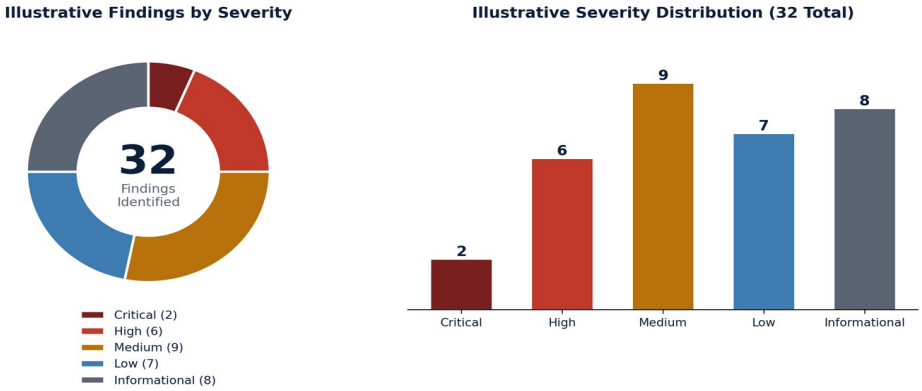
ALL METRICS, FINDINGS, AND SCORES ON THIS PAGE ARE ILLUSTRATIVE SAMPLE DATA

Overall Illustrative Security Posture

REQUIRES REMEDIATION

NorthStar's simulated web application demonstrates a number of established security controls, but the fictional assessment identified material weaknesses in authorization, business-logic enforcement, and account-recovery workflows that require prioritized remediation before the application should be considered ready for a broader trust posture. This illustrative status reflects a sample penetration-testing exercise and does not represent a certification or compliance decision.

Fictional Sample Dashboard



Illustrative severity distribution across all 32 fictional findings — ILLUSTRATIVE SAMPLE DATA.

Executive Risk Narrative

The fictional assessment identified 32 illustrative findings across the NorthStar Commerce Portal: 2 Critical, 6 High, 9 Medium, 7 Low, and 8 Informational. The two Critical findings concern business-logic and authorization exposure — a cross-tenant object-level authorization gap allowing access to another fictional customer's organization data, and a subscription-tier escalation path that bypasses payment authorization. Both represent the type of foundational trust-boundary failure that TMG Security prioritizes for immediate remediation in any real engagement of this kind.

The six High findings span stored cross-site scripting in the support workflow, an account-recovery weakness that could allow unauthorized email changes, server-side request forgery in the webhook-validation feature, a privilege-escalation path from Standard User to Organization Manager, excessive API data exposure on the organization-members endpoint, and a file-download authorization bypass. Together with the Critical findings, these High-severity issues concentrate around authorization enforcement and trust-boundary validation — a common and expected pattern for a multi-tenant SaaS application undergoing its first thorough offensive-security assessment.

Medium-severity findings reflect defense-in-depth gaps — rate limiting, session-revocation timing, CORS scope, verbose error handling, mass assignment, webhook replay protection, file-content validation, and a business-logic replay condition in the discount-redemption workflow. Low and Informational findings are hardening opportunities — version disclosure, header coverage, documentation accuracy, and monitoring enhancements — that support a stronger long-term security posture without representing an immediate exploitation path in this fictional sample.

TMG Security's simulated recommendation is that NorthStar prioritize closure of the two Critical and six High findings within the first 60 days of the illustrative remediation roadmap (see Section 42), with Medium findings addressed within 90 days and Low/Informational items folded into the ongoing defense-in-depth backlog. A full retest is recommended following remediation of all Critical and High findings, per the retest methodology in Section 44.

04 ENGAGEMENT OVERVIEW

This section describes the fictional objective, type, and approach of the illustrative NorthStar Commerce Portal web application penetration test, prepared to demonstrate TMG Security's engagement-scoping and reporting standards.

Assessment Objective

The fictional objective of this engagement was to identify and validate exploitable security weaknesses across the NorthStar Commerce Portal's authentication, authorization, business-logic, API, and infrastructure-adjacent surfaces, and to provide NorthStar's engineering leadership with prioritized, actionable remediation guidance.

Assessment Type & Testing Window

This is a fictional Web Application Penetration Test conducted against a controlled, fictional staging environment over the illustrative assessment period of 01 August 2026 – 31 August 2026, with this report issued 10 September 2026.

Testing Approach

- Authenticated testing across all six fictional application roles (Unauthenticated Visitor, Standard User, Billing User, Organization Manager, Support Agent, Administrator).
- Unauthenticated testing of all publicly reachable fictional endpoints and workflows.
- Role-based testing designed to independently validate both horizontal and vertical authorization boundaries.
- Business-logic analysis of fictional multi-step workflows (subscription changes, discount redemption, account recovery, invitation acceptance).
- API-assisted testing of the fictional web-service layer supporting the application, including object- and function-level authorization.

This engagement overview describes a fictional, illustrative assessment. No real client engagement occurred.

05 APPLICATION PROFILE

NorthStar Commerce Portal is a fictional enterprise SaaS application created to demonstrate a realistic assessment scope. All organization, technology, and infrastructure detail below is illustrative.

Fictional Client Profile

Attribute	Detail
Organization	NorthStar Digital Commerce, Inc. (Fictional)
Industry	E-Commerce / SaaS / Digital Payments
Headquarters	Austin, Texas, USA (Fictional)
Employees	Approximately 650 (Fictional)
Registered Users	Approximately 1.8 million (Fictional)
Application Name	NorthStar Commerce Portal (Fictional)
Application URL	https://portal.northstar-example.com (Fictional, non-resolving placeholder)
Environment	Fictional staging / controlled assessment environment

Application Capabilities (Fictional)

- User registration, login, and multi-factor authentication
- Password reset and account recovery
- User profile and organization management, including team members and role management
- Invoices, subscription management, and payment history
- File uploads (support attachments, invoice documents)
- Support ticketing and in-app notifications
- API integrations and outbound webhooks

- Administrative dashboard for platform-wide management

Fictional User Roles

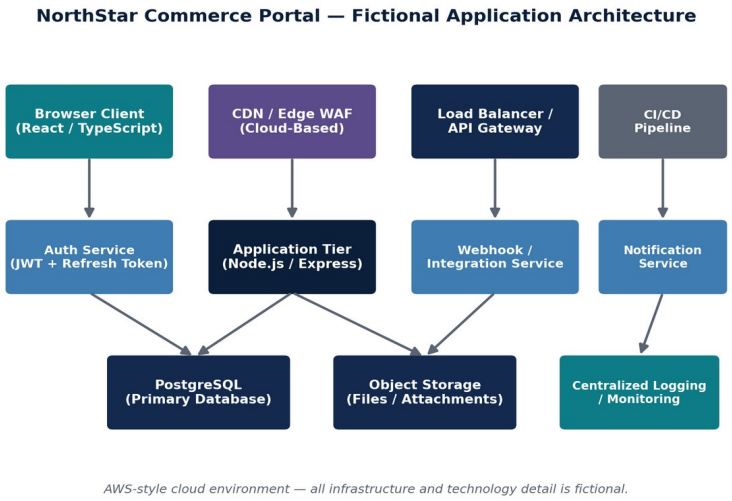
#	Role	Illustrative Description
1	Unauthenticated Visitor	Public marketing pages, registration, login, password reset.
2	Standard User	Default authenticated role; personal profile, files, support tickets.
3	Billing User	Standard User privileges plus billing, invoices, and subscription management.
4	Organization Manager	Organization profile, member/role management, webhook configuration.
5	Support Agent	Internal role; support-ticket queue and customer-facing ticket resolution.
6	Administrator	Platform-wide administrative dashboard and cross-organization management.

Fictional Technology Stack

Layer	Fictional Technology
Frontend	React / TypeScript
Backend	Node.js / Express
Database	PostgreSQL
Authentication	JWT (access token) + rotating refresh-token architecture
Infrastructure	AWS-style cloud environment (fictional)
CDN / WAF	Cloud-based edge protection (fictional)
Storage	Object-storage service (fictional)
CI/CD	Git-based deployment pipeline (fictional)

All infrastructure and technology detail above is fictional and provided only to give this sample report realistic structure and depth.

Fictional Application Architecture



Illustrative fictional application architecture — all infrastructure and technology detail is fictional.

06 TESTING SCOPE

The following fictional scope table defines the boundaries of this illustrative assessment.

In Scope

Area	Detail
Web Application	NorthStar Commerce Portal front-end and supporting API (fictional)
Authentication	Login, registration, MFA, session issuance and management
Account Management	Profile, password reset, account recovery, email change
Authorization	Role enforcement, object- and function-level access control
File Upload	Support and invoice attachment upload/download workflows
Organization Management	Organization profile, member management, role assignment
Billing Workflows	Invoices, payment history
Subscription Workflows	Plan changes, discount redemption
Support Tickets	Ticket creation, comments, internal agent views
Notification Systems	In-app notification generation and delivery
Web APIs	All /api/v1/* endpoints supporting the application
Webhooks	Webhook configuration, validation, and delivery

Out of Scope

Area	Detail
Denial-of-Service Testing	Not performed under any circumstances
Destructive Testing	Not performed under any circumstances
Social Engineering	Not included in this engagement
Physical Security	Not included in this engagement
Production Infrastructure	Testing restricted to the fictional staging environment only
Third-Party Systems	Not tested; only NorthStar-owned fictional application surface in scope
Cloud Provider Internals	Underlying cloud-provider infrastructure not tested

07 RULES OF ENGAGEMENT

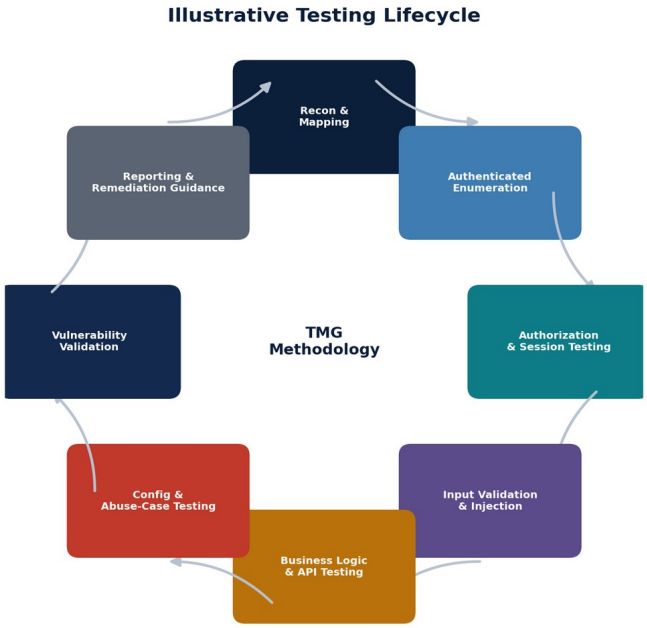
The following fictional rules of engagement governed this illustrative assessment and are representative of the controls TMG Security applies to every real engagement.

- All testing was controlled, authenticated where applicable, and performed only against the designated fictional staging environment.
- All testing was strictly non-destructive; no data-modifying action was taken outside of dedicated fictional test objects.
- Testing used only the dedicated fictional test accounts listed in Appendix D — no real user accounts or real customer data were used at any point.
- All evidence (fictional) was preserved in a structured evidence register (Appendix B / Section 48-equivalent evidence references) for traceability.
- No persistence mechanisms, backdoors, or long-lived footholds were established at any point.
- No destructive actions (data deletion, service disruption) were taken or simulated as executed.
- All automated testing respected reasonable request-rate limits; no denial-of-service condition was induced.
- No real customer data was accessed, used, or referenced at any point in this fictional engagement.
- Defined stop conditions applied: testing would have paused immediately upon any unexpected impact indicator, with emergency escalation to the fictional NorthStar engineering point of contact.

These rules of engagement are illustrative and describe the fictional engagement model used to construct this sample report.

08 METHODOLOGY

TMG Security's web application penetration-testing methodology follows a mature, staged process, conceptually informed by industry-recognized testing frameworks including the OWASP Web Security Testing Guide, the OWASP Top 10, and the OWASP API Security Top 10. No copyrighted material from these references is reproduced in this report; they are cited only as conceptual grounding for TMG Security's own methodology.



Illustrative TMG Security testing lifecycle applied to this fictional assessment.

Methodology Stages

#	Stage	Illustrative Description
1	Reconnaissance	Passive and light active information gathering on the fictional target.
2	Attack Surface Mapping	Enumeration of fictional endpoints, roles, and workflows.
3	Application Enumeration	Systematic walkthrough of fictional application functionality by role.
4	Authentication Testing	Login, MFA, password-reset, and session-issuance assessment.
5	Authorization Testing	Horizontal and vertical access-control validation.
6	Session Management	Token lifecycle, revocation, and fixation/hijacking resistance.
7	Input Validation	Boundary, format, and malformed-input handling.
8	Injection Testing	SQL/NoSQL/command/template/XSS-class testing using safe fictional payloads.
9	Business Logic	Workflow-state and process-integrity testing.
10	File Handling	Upload validation, storage, and download-authorization testing.
11	API Testing	Object- and function-level authorization, data exposure, rate limiting.
12	Configuration Testing	Headers, TLS, HTTP methods, default/debug endpoints.
13	Client-Side Testing	DOM-based issues, storage, source maps, front-end secrets.
14	Server-Side Testing	Server-side authorization, error handling, framework hardening.
15	Abuse-Case Testing	Rate limiting, race conditions, workflow abuse.
16	Vulnerability Validation	Manual confirmation of every candidate finding before inclusion.
17	Risk Assessment	Illustrative CVSS-inspired scoring and business-impact mapping.
18	Reporting	Structured finding documentation per Section 45 (Finding Format).
19	Remediation Guidance	Prioritized, actionable recommendations per finding.
20	Retest Recommendations	Defined retest scope and closure criteria (Section 44).

09 RISK RATING METHODOLOGY

TMG Security assigns each finding a severity rating using language inspired by the CVSS v3.1 scoring framework, considering exploitability, privileges required, user interaction, and technical/business impact. All scores in this report are illustrative and were assigned for this fictional sample only.

Severity Definitions

Severity	Illustrative Score Range	Definition
CRITICAL	9.0 – 10.0	Directly exploitable with severe confidentiality, integrity, or availability impact; typically requires immediate remediation.
HIGH	7.0 – 8.9	Significant impact with limited prerequisites; requires prompt remediation.
MEDIUM	4.0 – 6.9	Moderate impact, often requiring specific conditions or providing defense-in-depth value when fixed.
LOW	0.1 – 3.9	Minor impact; hardening opportunity rather than a directly exploitable weakness.
INFORMATIONAL	N/A	Observation or recommendation with no direct security-control failure.

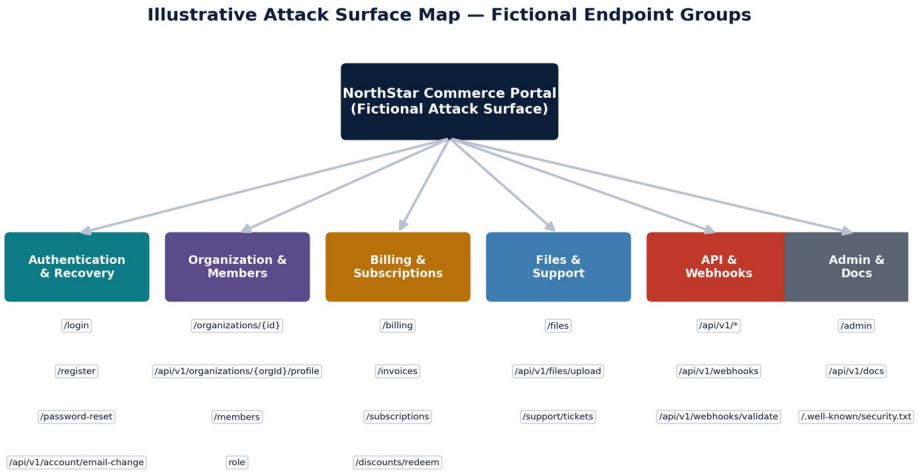
Rating Factors Considered

- Exploitability — how readily the fictional weakness could be exercised.
- Privileges Required — the level of fictional access needed before the weakness is reachable.
- User Interaction — whether a fictional victim action is required.
- Attack Complexity — conditions beyond the attacker's control that must align.
- Technical Impact — effect on confidentiality, integrity, and availability.
- Business Impact — fictional effect on revenue, fraud exposure, customer trust, and regulatory posture.

IMPORTANT: All CVSS-style scores, severities, and risk ratings in this report are fictional and illustrative.

10 ATTACK SURFACE MAPPING

TMG Security mapped the fictional NorthStar Commerce Portal's attack surface across six functional groups before beginning role-based testing. The full 34-endpoint register is provided in Appendix B (Section 48); a representative summary is shown here.



Illustrative attack-surface map — fictional endpoint groups and representative routes.

Representative Fictional Endpoints

Endpoint	Method	Auth
/login	POST	None
/register	POST	None
/api/v1/organizations/{orgId}/profile	GET / PATCH	Session
/api/v1/organizations/{orgId}/members/{userId}/role	PATCH	Session
/api/v1/billing/subscriptions/{subId}/plan	POST	Session
/api/v1/files/{fileId}/download	GET	Session
/api/v1/webhooks/validate	POST	Session
/api/v1/support/tickets/{id}/comments	POST	Session
/admin	GET	Session (Administrator)

A complete inventory of all 34 fictional endpoints — including method, required authentication, associated role, and testing result — is provided in Appendix B — Endpoint Register (Section 48).

11 RECONNAISSANCE SUMMARY

Reconnaissance for this fictional assessment combined passive observation of publicly reachable resources with light active enumeration of the staging environment, consistent with the non-destructive rules of engagement in Section 07.

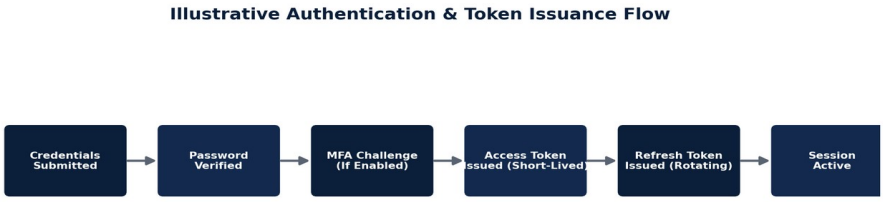
Fictional Reconnaissance Activities

- Passive review of publicly reachable pages, robots.txt, and the fictional API documentation endpoint.
- Technology fingerprinting via response headers, error signatures, and front-end bundle structure (see TMG-WAPT-018, TMG-WAPT-027).
- Enumeration of the fictional application's role structure via the six provided test accounts (Appendix D).
- Mapping of the fictional API surface via authenticated browsing and the interactive documentation endpoint.
- Identification of the fictional webhook and file-handling features as candidates for deeper server-side testing.

Illustrative Observations

Reconnaissance confirmed a conventional single-page-application architecture backed by a versioned REST API, consistent with the fictional technology stack described in Section 05. No unexpected or undocumented fictional subdomains or shadow endpoints were identified during this phase.

12 AUTHENTICATION TESTING



Illustrative authentication and token-issuance flow.

TMG Security assessed the fictional login, registration, password-policy, and account-verification workflows for weaknesses in credential handling, brute-force resistance, and account-enumeration exposure.

Illustrative Tests Performed

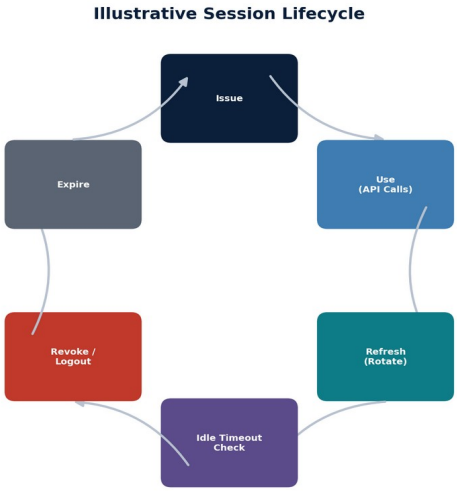
- Login rejects invalid credentials with a generic, non-distinguishing error message.
- Account lockout / throttling activates after repeated fictional failed login attempts.
- Password-complexity policy is enforced server-side, independent of client-side validation.
- Registration workflow does not leak account-existence signals through response timing or content.
- Email-verification step cannot be bypassed via direct API state manipulation.

Illustrative Observations

Fictional login-throttling and generic-error behavior were found adequate. One Low-severity observation (TMG-WAPT-019) noted that the registration workflow's validation messaging distinguishes an already-registered fictional email from a malformed one, a minor account-enumeration signal addressed alongside this section.

Finding ID	Severity	Title
TMG-WAPT-019	LOW	Verbose Validation Response

13 SESSION MANAGEMENT TESTING



Illustrative session lifecycle.

TMG Security assessed fictional cookie/token security attributes, refresh-token rotation, logout invalidation, and resistance to session fixation and hijacking.

Illustrative Tests Performed

- Session cookie carries Secure, HttpOnly, and SameSite attributes.
- Refresh-token rotation invalidates the prior token on each use.
- Logout invalidates the refresh token and, ideally, the current access token.
- Concurrent-session behavior across multiple fictional devices matches documented policy.
- Session identifiers are regenerated at authentication to resist fixation.

Illustrative Observations

Refresh-token rotation and cookie attributes were implemented soundly in the fictional environment. Two Medium/Low findings were identified: access tokens remain valid for their full lifetime after logout rather than being actively revoked (TMG-WAPT-010), and one non-privileged local-storage artifact persists after logout (TMG-WAPT-022).

Finding ID	Severity	Title
TMG-WAPT-010	MEDIUM	JWT / Session Revocation Weakness
TMG-WAPT-022	LOW	Logout Does Not Immediately Clear One Non-Privileged Local Session Artifact

14 AUTHORIZATION TESTING

Illustrative fictional role hierarchy.

Authorization testing was one of the most detailed testing categories in this fictional assessment, covering horizontal privilege escalation, vertical privilege escalation, and server-side enforcement of role boundaries across all six fictional user roles.

Illustrative Tests Performed

- Horizontal privilege escalation between fictional test tenants on organization-scoped objects.
- Vertical privilege escalation from Standard User toward Organization Manager and Administrator functions.
- Server-side authorization enforcement independent of front-end role-based UI hiding.
- Role-change and permission-grant endpoints validated for requester-role authorization.
- Cross-tenant isolation validated across organization, billing, and file-scoped fictional objects.

Illustrative Observations

This category produced the fictional assessment's most significant results: a Critical cross-tenant object-level authorization gap (TMG-WAPT-001) and a High-severity self-role-elevation path from Standard User to Organization Manager (TMG-WAPT-006). Both point to a systemic pattern — authorization enforced at the "is authenticated" level rather than the "is this specific action/object authorized for this specific requester" level — addressed further in the Attack Chain Analysis (Section 40).

Finding ID	Severity	Title
TMG-WAPT-001	CRITICAL	Broken Object-Level Authorization Leading to Cross-Tenant Customer Data Access
TMG-WAPT-006	HIGH	Privilege Escalation from Standard User to Organization Manager

15 ACCESS CONTROL TESTING

Access control testing focused on direct object references and function-level access restrictions across the fictional file-management and administrative surfaces, closely related to, but distinct from, the broader authorization testing in Section 14.

Illustrative Tests Performed

- Direct object references (file IDs) tested for cross-tenant accessibility.
- Administrative dashboard routes tested for accessibility without an Administrator session.
- Signed download-URL issuance tested for ownership verification.
- Function-level access control tested on privileged, non-role-change administrative actions.

Illustrative Observations

A High-severity file-download authorization bypass was identified (TMG-WAPT-008), structurally similar to the Critical cross-tenant finding in Section 14 — both stem from missing object-ownership verification prior to serving fictional data or documents.

Finding ID	Severity	Title
TMG-WAPT-008	HIGH	File Download Authorization Bypass

16 INPUT VALIDATION & INJECTION TESTING

TMG Security tested the fictional application's handling of malformed, oversized, and adversarial input, including safe illustrative payloads representative of SQL injection, NoSQL injection, command injection, template injection, path traversal, and cross-site scripting classes.

Illustrative Tests Performed

- SQL- and NoSQL-injection-style fictional payloads submitted to search/filter parameters.
- OS command-injection-style fictional payloads submitted to file-name and metadata fields.
- Server-side template-injection-style fictional payloads submitted to user-supplied text fields.
- Path-traversal-style fictional payloads submitted to file-reference parameters.
- Stored HTML/script content submitted to the support-ticket comment field, then reviewed across all rendering contexts.

Illustrative Observations

Parameterized data access appeared consistently applied across the fictional data layer; no SQL/NoSQL/command/template-injection-class weakness was identified. One High-severity stored cross-site-scripting finding was confirmed in the support-ticket comment workflow (TMG-WAPT-003), where output encoding was inconsistently applied between the customer-facing and internal Support Agent rendering paths.

Finding ID	Severity	Title
TMG-WAPT-003	HIGH	Stored Cross-Site Scripting in Customer Support Workflow

17 BUSINESS LOGIC TESTING

Business-logic testing examined the fictional application's multi-step workflows — subscription changes, discount redemption, invoice state transitions, and account-ownership changes — for state-manipulation and workflow-integrity weaknesses that conventional input-validation testing does not surface.

Illustrative Tests Performed

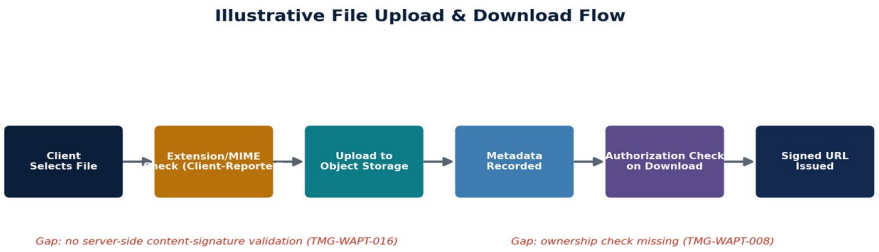
- Subscription plan-tier transitions tested for reliance on client-supplied authorization state.
- Single-use discount-code redemption tested for repeat/replay redemption.
- Invoice state-transition order tested for workflow-skipping.
- Email-verification and account-ownership workflows tested for state-manipulation bypass.
- Notification-triggering events cross-checked against actual enforcement state.

Illustrative Observations

This category produced the fictional assessment's second Critical finding: subscription plan-tier escalation that bypasses the expected server-side payment-authorization step (TMG-WAPT-002). A related Medium-severity business-logic replay condition was also confirmed in the discount-redemption workflow (TMG-WAPT-017), where a narrow validation window allowed a single-use code to be redeemed twice.

Finding ID	Severity	Title
TMG-WAPT-002	CRITICAL	Business Logic Authorization Bypass Allowing Unauthorized Subscription Privilege Escalation
TMG-WAPT-017	MEDIUM	Business Logic Replay in Discount Workflow

18 FILE UPLOAD & FILE HANDLING



Illustrative file upload and download flow, showing the two identified gaps.

TMG Security assessed fictional file-type validation, storage handling, filename sanitization, and download-authorization controls across the support-attachment and invoice-document upload features.

Illustrative Tests Performed

- File-type validation tested for reliance on client-supplied extension/MIME-type versus server-side content inspection.
- Filename handling tested for path-traversal characters.
- Storage location tested for direct, unauthenticated object-storage accessibility.
- Download-authorization tested for cross-tenant object-ownership verification.

Illustrative Observations

Server-side content-type validation was found insufficient — a fictional test file with a mismatched extension and declared MIME type was accepted (TMG-WAPT-016). Download-authorization is covered under the related Access Control finding (TMG-WAPT-008, Section 15).

Finding ID	Severity	Title
TMG-WAPT-016	MEDIUM	Insufficient File Validation

19 PASSWORD RESET & ACCOUNT RECOVERY

TMG Security assessed the fictional password-reset and account-recovery workflows for token-handling weaknesses, rate-limiting gaps, and email-change abuse potential.

Illustrative Tests Performed

- Password-reset tokens tested for expiration window and single-use enforcement.
- Password-reset-request endpoint tested for application-level rate limiting.
- Email-change confirmation codes tested for binding to their originating change-request.
- Account-recovery workflow tested end-to-end for takeover-risk conditions.

Illustrative Observations

Token expiration and single-use enforcement were adequate in the fictional environment. Two findings were identified: insufficient rate limiting on the password-reset-request endpoint (TMG-WAPT-009, Medium), and a High-severity weakness

in the email-change confirmation flow where a confirmation code was not bound to its specific originating request (TMG-WAPT-004).

Finding ID	Severity	Title
TMG-WAPT-004	HIGH	Account Recovery Workflow Allows Unauthorized Email Change
TMG-WAPT-009	MEDIUM	Insufficient Rate Limiting on Password Reset Endpoint

20 MFA & ACCOUNT SECURITY

TMG Security assessed the fictional multi-factor authentication implementation for privileged roles, including enrollment, challenge enforcement, recovery-code handling, and remembered-device duration.

Illustrative Tests Performed

- MFA enforced at login for fictional accounts with MFA enabled, with no observable bypass path.
- MFA enrollment available and functional for Administrator and Organization Manager roles.
- MFA recovery-code usage tested for single-use enforcement and logging.
- "Remembered device" duration tested for a bounded, independently configurable window.

Illustrative Observations

MFA enforcement, recovery-code handling, and remembered-device duration were all found adequate in the fictional test environment. This is a positive control observation — see Section 45.

No findings raised against this fictional testing category beyond items cross-referenced elsewhere in this report.

21 API & WEB SERVICE TESTING

Because the fictional NorthStar Commerce Portal is API-driven, TMG Security applied dedicated API-security testing informed by the OWASP API Security Top 10 categories — authentication, authorization (BOLA/BFLA), excessive data exposure, mass assignment, and rate limiting — without reproducing copyrighted category text.

Illustrative Tests Performed

- Object-level authorization (BOLA) validated across all organization- and file-scoped API endpoints.
- Function-level authorization validated on privileged API actions.
- API response payloads reviewed for excessive data exposure relative to requester role.
- Request bodies reviewed for mass-assignment exposure of internal-only fields.
- API error-handling reviewed for consistent, non-verbose responses.

Illustrative Observations

Two findings specific to the API layer were confirmed: excessive data exposure through the organization-members endpoint (TMG-WAPT-007, High) and mass assignment in the organization-profile update endpoint (TMG-WAPT-014, Medium). Object- and function-level authorization findings for this layer are detailed in Sections 14 and 15.

Finding ID	Severity	Title
TMG-WAPT-007	HIGH	Excessive API Data Exposure Through Organization Endpoint
TMG-WAPT-014	MEDIUM	Mass Assignment in Organization Profile Update

22 CORS / SECURITY HEADERS / BROWSER SECURITY

TMG Security reviewed the fictional application's CORS configuration and browser-security response headers, including CSP, HSTS, X-Content-Type-Options, frame protection, and Referrer-Policy, and assessed sensitive-token handling in browser storage.

Illustrative Tests Performed

- CORS Access-Control-Allow-Origin reviewed for scope against the active front-end origin set.
- Access-Control-Allow-Credentials reviewed in combination with the CORS origin policy.
- Content-Security-Policy, X-Frame-Options/frame-ancestors, HSTS, and X-Content-Type-Options presence reviewed.
- Referrer-Policy and Permissions-Policy presence reviewed.
- Browser storage reviewed for sensitive-token exposure.

Illustrative Observations

Several defense-in-depth gaps were identified: an overly broad CORS allow-list (TMG-WAPT-011, Medium), absence of a Content-Security-Policy and inconsistent frame protection (TMG-WAPT-013, Medium), and missing Referrer-Policy (TMG-WAPT-020, Low) and Permissions-Policy (TMG-WAPT-028, Informational) headers. Sensitive tokens were not found stored in cleartext browser storage.

Finding ID	Severity	Title
TMG-WAPT-011	MEDIUM	CORS Trusts Unnecessary Origins
TMG-WAPT-013	MEDIUM	Missing Security Header Defense
TMG-WAPT-020	LOW	Missing Referrer-Policy Hardening
TMG-WAPT-028	INFORMATIONAL	Unused Security Response Header Opportunity

23 SSRF & SERVER-SIDE REQUEST HANDLING

TMG Security assessed the fictional webhook-validation feature — the only server-side URL-fetching functionality identified in this application — for server-side request forgery (SSRF) exposure, using only safe, attacker-controlled test endpoints and never attempting to reach internal or metadata addresses.

Illustrative Tests Performed

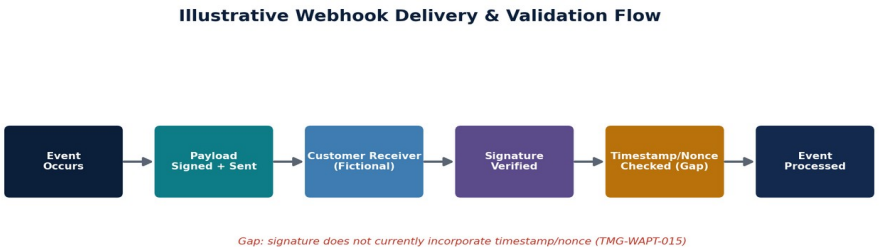
- Webhook-validation feature tested with an attacker-controlled, non-destructive fictional observer endpoint.
- Outbound request destination reviewed for egress allow-listing / private-range blocking.
- DNS-resolution behavior reviewed for redirect-based SSRF potential (not exploited, reviewed only).

Illustrative Observations

A High-severity SSRF-class weakness was confirmed in the webhook-validation feature (TMG-WAPT-005): the fictional server issued an outbound request to an attacker-controlled test endpoint with no observed destination restriction. Consistent with the non-destructive rules of engagement, this assessment did not attempt to reach any internal network range or cloud metadata endpoint.

Finding ID	Severity	Title
TMG-WAPT-005	HIGH	Server-Side Request Forgery in Webhook Validation Feature

24 WEBHOOK SECURITY



Illustrative webhook delivery and validation flow, showing the replay-protection gap.

TMG Security assessed the fictional outbound webhook-delivery mechanism for signature validation, replay protection, event authentication, and duplicate-event handling.

Illustrative Tests Performed

- Outbound webhook payloads verified to carry a signature.
- Signature scheme reviewed for timestamp/nonce-based replay protection.
- Captured fictional payloads replayed to test signature-validation reuse.
- Webhook configuration access restricted to Organization Manager and Administrator roles.

Illustrative Observations

Signature validation was present but did not incorporate a timestamp or nonce, allowing a captured fictional payload to pass validation again on replay (TMG-WAPT-015, Medium). Webhook-configuration access control was found appropriately restricted.

Finding ID	Severity	Title
TMG-WAPT-015	MEDIUM	Webhook Replay Protection Missing

25 RATE LIMITING & ABUSE CONTROLS

TMG Security assessed fictional rate-limiting coverage across login, password reset, OTP/MFA, registration, invitation, and expensive API operations, using controlled request counts consistent with the non-destructive rules of engagement.

Illustrative Tests Performed

- Login endpoint tested for throttling with exponential backoff.
- Password-reset-request endpoint tested for per-account and per-source rate limiting.
- Registration and invitation endpoints tested for reasonable request-volume limits.
- Expensive API operations (report generation, bulk export) tested for request throttling.

Illustrative Observations

Login-endpoint rate limiting was found adequate. The password-reset-request endpoint permitted a fictional burst of 50 sequential requests without triggering application-level throttling (TMG-WAPT-009, Medium).

Finding ID	Severity	Title
TMG-WAPT-009	MEDIUM	Insufficient Rate Limiting on Password Reset Endpoint

26 CLIENT-SIDE SECURITY

TMG Security reviewed the fictional front-end bundle for DOM-based issues, sensitive information in JavaScript, insecure local-storage use, exposed source maps, and reliance on client-side authorization assumptions.

Illustrative Tests Performed

- Front-end bundle reviewed for source maps published to production.
- Browser local storage reviewed for sensitive tokens or credentials.
- Front-end bundle reviewed for residual debug logging.
- Client-side role checks cross-checked against equivalent server-side enforcement.

Illustrative Observations

No DOM-based XSS or exposed production source maps were identified. Residual client-side debug logging was found on a subset of pages (TMG-WAPT-021, Low), and client-side role checks were confirmed to require equivalent server-side enforcement per the API findings in Section 21.

Finding ID	Severity	Title
TMG-WAPT-021	LOW	Unnecessary Client-Side Debug Logging

27 SERVER-SIDE SECURITY

TMG Security reviewed fictional server-side authorization enforcement, framework default/debug behavior, exposed administrative interfaces, and HTTP-method handling.

Illustrative Tests Performed

- Framework default/debug endpoints tested for accessibility in the fictional staging configuration.
- Administrative interfaces tested for network- and authentication-level exposure.
- HTTP method enumeration performed against a representative sample of fictional endpoints.
- Server-side authorization independently verified for every privileged action identified during testing.

Illustrative Observations

No accessible framework debug endpoints were identified. Method enumeration found TRACE enabled by default on a subset of endpoints (TMG-WAPT-024, Low). Server-side authorization gaps identified during this testing are detailed under Authorization Testing (Section 14).

Finding ID	Severity	Title
TMG-WAPT-024	LOW	Security Configuration Hardening Opportunity

28 SENSITIVE DATA EXPOSURE

TMG Security reviewed fictional API responses, debug output, and metadata for exposure of user information, organization information, invoice data, internal identifiers, and stack traces. No real personal data was accessed or referenced at any point.

Illustrative Tests Performed

- API responses reviewed for over-inclusion of internal or billing-linked fields.
- Debug and error output reviewed for stack traces or internal identifiers.
- File metadata reviewed for unintended internal-note exposure.
- Front-end bundle reviewed for embedded internal identifiers or configuration.

Illustrative Observations

The excessive API data exposure identified on the organization-members endpoint (TMG-WAPT-007, Section 21) is the primary sensitive-data-exposure finding in this fictional assessment. No exposure of fictional user personal information beyond the scoped test-account data was identified.

Finding ID	Severity	Title
TMG-WAPT-007	HIGH	Excessive API Data Exposure Through Organization Endpoint

29 ERROR HANDLING & INFORMATION DISCLOSURE

TMG Security submitted malformed and boundary-condition input across the fictional API surface to assess error-handling consistency and information-disclosure exposure.

Illustrative Tests Performed

- Malformed JSON and oversized payloads submitted to representative endpoints.
- Error responses reviewed for stack traces, internal file paths, or ORM query fragments.
- Response headers reviewed for framework/version disclosure.
- Registration validation messaging reviewed for account-enumeration signals.

Illustrative Observations

Verbose error responses containing internal exception detail were confirmed on several fictional endpoints (TMG-WAPT-012, Medium). Related, lower-severity observations include technology version disclosure (TMG-WAPT-018, Low) and distinguishable registration validation messaging (TMG-WAPT-019, Low).

Finding ID	Severity	Title
TMG-WAPT-012	MEDIUM	Verbose Error Messages Reveal Internal Application Details
TMG-WAPT-018	LOW	Technology Version Disclosure
TMG-WAPT-019	LOW	Verbose Validation Response

30 SECURITY CONFIGURATION

TMG Security reviewed fictional HTTP method handling, cookie configuration, TLS configuration, directory listing, default endpoints, and exposed documentation.

Illustrative Tests Performed

- HTTP method enumeration across a representative sample of endpoints.
- TLS configuration reviewed for deprecated protocol versions and weak cipher suites.
- Static-asset paths reviewed for directory listing.
- Vulnerability-disclosure metadata (security.txt) reviewed for presence.

Illustrative Observations

TLS configuration and directory-listing controls were found adequate. Unused HTTP methods were found enabled by default on a subset of endpoints (TMG-WAPT-024, Section 27), and no security.txt file was published (TMG-WAPT-025, Informational).

Finding ID	Severity	Title
TMG-WAPT-025	INFORMATIONAL	Security.txt Not Present

31 RACE CONDITIONS / CONCURRENCY

TMG Security performed controlled, safe concurrency testing against fictional workflows with single-use or state-transition semantics — discount redemption, invitation acceptance, and subscription state transitions — using synthetic, rate-limited request pairs rather than high-volume automation.

Illustrative Tests Performed

- Rapid-sequence discount-code redemption tested against the same fictional single-use code.
- Concurrent invitation-acceptance requests tested against the same fictional invitation token.
- Concurrent subscription state-transition requests tested for atomicity.

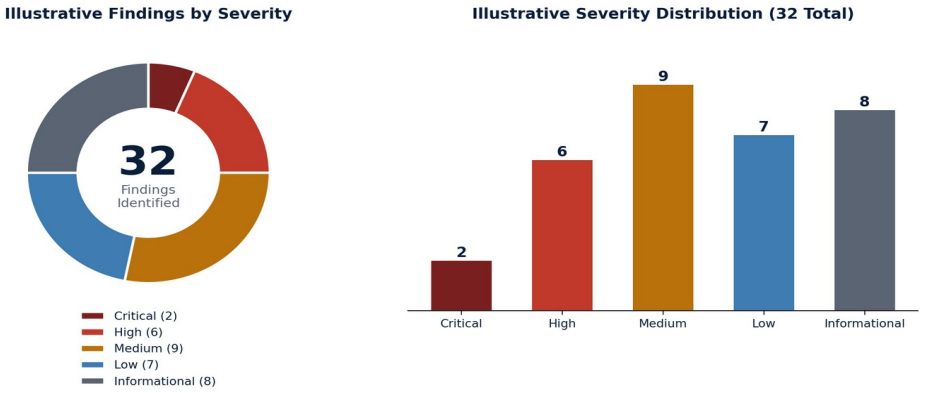
Illustrative Observations

A Medium-severity business-logic replay condition was confirmed in the discount-redemption workflow, where two rapid-sequence requests both succeeded against the same single-use fictional code (TMG-WAPT-017). No race-condition weakness was identified in invitation acceptance or subscription state transitions beyond the business-logic issue already described in Section 17.

Finding ID	Severity	Title
TMG-WAPT-017	MEDIUM	Business Logic Replay in Discount Workflow

32 FINDINGS SUMMARY

This fictional assessment identified 32 illustrative findings across the NorthStar Commerce Portal, summarized below. Full detail for every finding, including safe proof-of-concept evidence, is provided in Sections 34-38, organized by severity.



Illustrative severity distribution — ILLUSTRATIVE SAMPLE DATA.

Findings at a Glance

Finding ID	Title	Severity
TMG-WAPT-001	Broken Object-Level Authorization Leading to Cross-Tenant Customer Data Access	CRITICAL
TMG-WAPT-002	Business Logic Authorization Bypass Allowing Unauthorized Subscription Privilege Escalation	CRITICAL
TMG-WAPT-003	Stored Cross-Site Scripting in Customer Support Workflow	HIGH
TMG-WAPT-004	Account Recovery Workflow Allows Unauthorized Email Change	HIGH
TMG-WAPT-005	Server-Side Request Forgery in Webhook Validation Feature	HIGH
TMG-WAPT-006	Privilege Escalation from Standard User to Organization Manager	HIGH
TMG-WAPT-007	Excessive API Data Exposure Through Organization Endpoint	HIGH
TMG-WAPT-008	File Download Authorization Bypass	HIGH
TMG-WAPT-009	Insufficient Rate Limiting on Password Reset Endpoint	MEDIUM
TMG-WAPT-010	JWT / Session Revocation Weakness	MEDIUM

Finding ID	Title	Severity
TMG-WAPT-011	CORS Trusts Unnecessary Origins	MEDIUM
TMG-WAPT-012	Verbose Error Messages Reveal Internal Application Details	MEDIUM
TMG-WAPT-013	Missing Security Header Defense	MEDIUM
TMG-WAPT-014	Mass Assignment in Organization Profile Update	MEDIUM
TMG-WAPT-015	Webhook Replay Protection Missing	MEDIUM
TMG-WAPT-016	Insufficient File Validation	MEDIUM
TMG-WAPT-017	Business Logic Replay in Discount Workflow	MEDIUM
TMG-WAPT-018	Technology Version Disclosure	LOW
TMG-WAPT-019	Verbose Validation Response	LOW
TMG-WAPT-020	Missing Referrer-Policy Hardening	LOW
TMG-WAPT-021	Unnecessary Client-Side Debug Logging	LOW
TMG-WAPT-022	Logout Does Not Immediately Clear One Non-Privileged Local Session Artifact	LOW
TMG-WAPT-023	Password Policy Documentation Inconsistency	LOW
TMG-WAPT-024	Security Configuration Hardening Opportunity	LOW
TMG-WAPT-025	Security.txt Not Present	INFORMATIONAL
TMG-WAPT-026	API Documentation Exposure — Intended but Reviewable	INFORMATIONAL
TMG-WAPT-027	Detailed Technology Fingerprinting	INFORMATIONAL
TMG-WAPT-028	Unused Security Response Header Opportunity	INFORMATIONAL
TMG-WAPT-029	Exposed Non-Sensitive Build Metadata	INFORMATIONAL
TMG-WAPT-030	Session Management Documentation Improvement	INFORMATIONAL
TMG-WAPT-031	Security Monitoring Enhancement Opportunity	INFORMATIONAL
TMG-WAPT-032	Defense-in-Depth Recommendation for Sensitive Workflows	INFORMATIONAL

33 DETAILED FINDINGS

The following sections (34-38) present each of the 32 fictional findings in full detail, grouped by severity: Critical, High, Medium, Low, and Informational. Every finding follows the consistent format defined below, and every Critical and High finding additionally includes a full illustrative evidence panel with fictional request/response detail.

Finding Format

Each finding card presents: Finding ID, Title, Severity, CVSS-style Score, CWE reference (where applicable), Affected Area, Affected Endpoint/Feature, Description, Business Context, Security & Technical Impact, Attack Prerequisites, a Safe Proof of Concept summary, Evidence Reference, Expected Behavior, Observed (Fictional) Behavior, Root Cause, Recommendation, Management Response, Owner/Priority/Target Date/Status, and a Retest Recommendation.

Safe Proof-of-Concept Standard

Every Proof of Concept in this report is illustrative and fictional. Requests use the placeholder domain https://portal.northstar-example.com, fictional bearer tokens shown as [FICTIONAL-TOKEN…], and synthetic test-user and object identifiers. No PoC in this report was executed against a real system, and none is destructive, weaponized, or intended to enable real-world exploitation.

ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE — every request, response, screenshot, and evidence reference in Sections 34-38 is synthetic.

34 CRITICAL FINDINGS

The following 2 fictional Critical-severity findings represent the assessment's highest-priority illustrative results.

TMG-WAPT-001 — Broken Object-Level Authorization Leading to Cross-Tenant Customer Data Access	CRITICAL
CVSS-Style Score: 9.1 (Critical) — Illustrative CVSS v3.1-inspired score	CWE: CWE-639 — Authorization Bypass Through User-Controlled Key
Affected Area	Organization Management / Multi-Tenant Data Isolation
Affected Endpoint / Feature	*GET /api/v1/organizations/{orgId}/profile*
Description	The organization-profile API endpoint accepts an org identifier supplied directly in the request path and returns the corresponding organization record without verifying that the requesting user's session is associated with that organization.
Business Context	NorthStar Commerce Portal is a multi-tenant SaaS platform; each customer organization's data (profile, members, billing metadata) must remain strictly isolated from every other tenant. Cross-tenant access is a foundational trust boundary for the platform.
Security & Technical Impact	Security Impact: an authenticated Standard User from one fictional test tenant was able to retrieve profile data belonging to a second, unrelated fictional test tenant by substituting the organization identifier. Technical Impact: the server performs no server-side ownership check between the authenticated session and the requested object, relying only on the client-supplied identifier.
Attack Prerequisites	A valid low-privilege authenticated session (e.g., Standard User) and knowledge or enumeration of a sequential/guessable organization identifier belonging to another tenant.
Safe Proof of Concept (Summary)	*Illustrative request substituting a foreign organization ID into an authenticated session returned that organization's fictional profile object instead of an authorization error. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-001, EV-WAPT-002 (redacted request/response capture, tenant-isolation test matrix)*
Expected Behavior	Server-side authorization should confirm the authenticated user's organization membership matches the requested organization ID before returning any data, independent of client-supplied values.
Observed (Fictional) Behavior	The endpoint trusted the path parameter alone and returned data for a fictional organization the authenticated test user did not belong to.
Root Cause	Missing server-side object-level authorization check; the endpoint authorizes on "is this a valid session" rather than "does this session own this specific object."
Recommendation	Enforce server-side tenant-scoping on every organization-scoped endpoint by deriving the organization context from the authenticated session (not the path/body), and add automated authorization regression tests for all object-level endpoints.
Management Response	*NorthStar engineering (fictional) has accepted this finding and will introduce a centralized tenant-scoping middleware validated in the 0-30 day remediation window, per the illustrative remediation roadmap in Section 42.*
Owner / Priority / Target / Status	**VP Engineering (Fictional Role)** | Immediate — 0-30 Days | 10 October 2026 | **Remediation In Progress**
Retest Recommendation	*Full retest required following remediation, including automated regression coverage across all organization-scoped endpoints and a manual cross-tenant verification pass.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
REQUEST (Fictional / Synthetic)
GET /api/v1/organizations/ORG-1002/profile HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-TESTUSER-1001]
X-Test-User: TEST-USER-1001 (member of ORG-1001)
Accept: application/json
```

```
RESPONSE (Fictional / Synthetic)
HTTP/1.1 200 OK
Content-Type: application/json

{
  "organization_id": "ORG-1002",
  "name": "NorthStar Demo Organization (Fictional Tenant B)",
  "status": "active",
  "billing_contact_email": "fictional.billing@example.test",
```

```
  "member_count": 14
}
```

Expected: The request should return HTTP 403 Forbidden because TEST-USER-1001 is a member of ORG-1001, not ORG-1002.

Observed: The application returned a fictional HTTP 200 response containing the profile object of an unrelated tenant, with no authorization error.

Impact: Cross-tenant object access at the API layer; if unaddressed, this class of issue could allow enumeration of other customers' fictional organization profile data.

TMG-WAPT-002 — Business Logic Authorization Bypass Allowing Unauthorized Subscription Privilege Escalation	**CRITICAL**
CVSS-Style Score: 9.0 (Critical) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-840 — Business Logic Errors**
Affected Area	Subscription Management / Entitlement Enforcement
Affected Endpoint / Feature	*POST /api/v1/billing/subscriptions/{subId}/plan*
Description	The subscription plan-change workflow accepts a client-supplied target plan tier and applies it without validating that the requesting user's role and the organization's payment state authorize the transition.
Business Context	Subscription tier directly gates premium application features and billing amount; unauthorized tier escalation represents both a revenue-integrity issue and unauthorized feature access.
Security & Technical Impact	Security Impact: a fictional Billing User account was able to escalate a test organization's subscription from "Standard" to "Enterprise" tier without a corresponding payment-authorization step. Technical Impact: entitlement flags controlling premium feature access are derived from the same unauthenticated-transition state, so the escalation immediately unlocked premium-tier functionality in the fictional test environment.
Attack Prerequisites	A valid Billing User (or equivalent) session within a test organization; no additional privilege is required.
Safe Proof of Concept (Summary)	*Illustrative plan-change request bypassing the expected payment-authorization/approval step and immediately elevating the fictional subscription tier. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-003, EV-WAPT-004 (redacted request/response capture, entitlement-flag comparison before/after)*
Expected Behavior	Plan-tier transitions should be authorized exclusively by a server-side payment/billing service event, never by a client-supplied boolean.
Observed (Fictional) Behavior	The client-supplied `payment_authorized` field was trusted directly by the plan-change handler.
Root Cause	Trust boundary violation — business-critical authorization state (payment verification) is accepted from the client instead of being derived server-side from the payments subsystem.
Recommendation	Remove client-controllable authorization fields from the request contract; require the plan-change handler to call the internal billing/payment verification service and gate all entitlement changes on its authoritative response.
Management Response	*NorthStar engineering (fictional) has prioritized this as a P0 item; a server-side entitlement gate keyed to the payments service is planned within the 0-30 day window.*
Owner / Priority / Target / Status	**Director, Billing Platform (Fictional Role)** | Immediate — 0-30 Days | 10 October 2026 | **Remediation In Progress**
Retest Recommendation	*Full retest required, including verification that plan-tier transitions cannot proceed without an authoritative server-side payment-verification event.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
REQUEST (Fictional / Synthetic)
POST /api/v1/billing/subscriptions/SUB-77421/plan HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-BILLINGUSER-2200]
Content-Type: application/json

{ "target_plan": "enterprise", "payment_authorized": true }
```

```
RESPONSE (Fictional / Synthetic)
HTTP/1.1 200 OK
Content-Type: application/json

{
```

```
  "subscription_id": "SUB-77421",
  "plan": "enterprise",
  "status": "active",
  "payment_verified": false
}
```

Expected: The server should reject or hold the transition pending a verified payment-authorization event from the payments subsystem before elevating the plan tier or enabling entitlements.

Observed: The fictional server accepted the client-supplied "payment_authorized" flag at face value and immediately activated the higher tier and its entitlements.

Impact: Unauthorized premium-tier feature access and potential fictional revenue-integrity impact if replicated across test organizations.

35 HIGH FINDINGS

The following 6 fictional High-severity findings should be prioritized immediately after the Critical findings in Section 34.

TMG-WAPT-003 — Stored Cross-Site Scripting in Customer Support Workflow	HIGH
CVSS-Style Score: 8.2 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-79 — Improper Neutralization of Input During Web Page Generation (XSS)**
Affected Area	Support Ticketing
Affected Endpoint / Feature	*POST /api/v1/support/tickets/{id}/comments*
Description	The support-ticket comment field does not sufficiently encode HTML/script content before it is rendered in the Support Agent and Administrator ticket-review views.
Business Context	Support Agents and Administrators routinely open customer-submitted tickets; a stored payload in a comment could execute in the context of a higher-privileged internal user reviewing the ticket.
Security & Technical Impact	Security Impact: a fictional payload submitted as a Standard User rendered as executable script in the fictional Support Agent view. Technical Impact: the application's output encoding on the ticket-comment rendering path is inconsistent between the customer-facing and internal-agent views.
Attack Prerequisites	A Standard User (or unauthenticated ticket-submission form, where enabled) able to submit ticket comment text; a Support Agent or Administrator must subsequently view the ticket.
Safe Proof of Concept (Summary)	*A fictional comment payload containing a benign, non-destructive marker script rendered unescaped in the internal support-agent ticket view. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-005 (fictional before/after rendering comparison, synthetic screenshot)*
Expected Behavior	All user-supplied ticket content should be encoded identically regardless of which role's view renders it.
Observed (Fictional) Behavior	Encoding was applied on the customer-facing view but not consistently on the internal Support Agent / Administrator view.
Root Cause	Inconsistent output-encoding implementation across two separate front-end rendering paths for the same underlying comment data.
Recommendation	Apply a single shared, context-aware output-encoding component across all ticket-rendering views; add a content-security-policy as defense-in-depth (see Section 22).
Management Response	*Accepted; the fictional front-end team will consolidate ticket-comment rendering onto the shared encoding component already used elsewhere in the application.*
Owner / Priority / Target / Status	**Engineering Lead, Support Platform (Fictional Role)** | 0-30 Days | 24 October 2026 | **Open**
Retest Recommendation	*Targeted retest of the ticket-comment rendering path across all roles after remediation.*

TMG-WAPT-004 — Account Recovery Workflow Allows Unauthorized Email Change	HIGH
CVSS-Style Score: 7.9 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-640 — Weak Password Recovery Mechanism**
Affected Area	Account Recovery
Affected Endpoint / Feature	*POST /api/v1/account/email-change*
Description	The email-change confirmation step accepts a confirmation code that is not bound to the specific email-change request that generated it, allowing an already-authenticated low-privilege session to complete an email change intended for a different, pending request.
Business Context	The account email address is a primary factor used later in password-reset and MFA-recovery workflows; unauthorized modification is a precursor to full account takeover.
Security & Technical Impact	Security Impact: in the fictional test environment, a confirmation code generated for one pending email-change request was accepted when submitted against a second, unrelated pending request on the same test account. Technical Impact: the confirmation-code validation checks only that the code is currently valid and unused, not that it matches the specific change-request ID it was issued for.
Attack Prerequisites	An authenticated session on the target test account and timing overlap between two pending email-change requests (achievable by initiating a second request before completing the first).
Safe Proof of Concept (Summary)	*Illustrative sequence showing a confirmation code issued for change-request A being accepted against change-request B on the same fictional account. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*

Evidence Reference	*EV-WAPT-006 (fictional request/response timeline)*
Expected Behavior	Confirmation-code validation should include the originating request identifier as part of the verification, not just code validity and expiry.
Observed (Fictional) Behavior	Code validation checked only value and expiry, not request binding.
Root Cause	Confirmation-code data model does not persist or check a request-scoped binding value.
Recommendation	Bind each confirmation code to its originating change-request ID and invalidate superseded pending requests when a new one is created for the same account.
Management Response	*Accepted; fictional identity-platform team will add request-scoped binding in the next sprint following the assessment period.*
Owner / Priority / Target / Status	**Identity & Access Lead (Fictional Role)** | 0-30 Days | 24 October 2026 | Open
Retest Recommendation	*Retest the full email-change and password-reset workflows together after remediation, including concurrent-request scenarios.*

TMG-WAPT-005 — Server-Side Request Forgery in Webhook Validation Feature	**HIGH**
CVSS-Style Score: 8.1 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-918 — Server-Side Request Forgery (SSRF)**
Affected Area	Webhook Configuration
Affected Endpoint / Feature	*POST /api/v1/webhooks/validate*
Description	The webhook "validate endpoint" feature, which performs a server-side test request to a customer-supplied callback URL before saving a webhook subscription, does not restrict the destination beyond basic URL-format validation.
Business Context	Organization Managers can register outbound webhook callback URLs for integration events; the validation feature is intended to confirm reachability before activation.
Security & Technical Impact	Security Impact: the fictional server was observed issuing an outbound request to an attacker-controlled observer endpoint supplied as the webhook URL, confirming the server performs the fetch itself rather than only validating URL syntax. Technical Impact: no destination allow-listing, DNS-resolution restriction, or private-IP-range blocking was observed in the fictional test environment.
Attack Prerequisites	An authenticated Organization Manager session able to configure a webhook, and a network-reachable listener to observe the callback (an attacker-controlled test endpoint in this illustrative case).
Safe Proof of Concept (Summary)	*A safe, non-destructive attacker-controlled test endpoint received a single fictional server-initiated request when submitted as the webhook target, confirming SSRF-class behavior without accessing any internal resource. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-007 (fictional observer-endpoint log, redacted request/response)*
Expected Behavior	Outbound validation requests should be restricted via an egress allow-list and should explicitly block RFC 1918 / link-local / metadata-service address ranges.
Observed (Fictional) Behavior	No such restriction was observed for the externally-routable test destination used in this illustrative assessment.
Root Cause	The webhook-validation feature performs a server-side fetch without a destination allow-list or private-range blocklist.
Recommendation	Implement an egress allow-list and explicit blocklist for private/link-local/metadata IP ranges on all server-initiated outbound fetches; consider routing validation requests through an isolated, non-privileged network egress path.
Management Response	*Accepted as a priority item; fictional platform-security team will implement destination filtering on the webhook-validation service.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 0-30 Days | 24 October 2026 | Remediation Planned
Retest Recommendation	*Retest with a broader set of safe, non-internal illustrative destinations to confirm the allow-list/blocklist behaves as expected; internal-range testing remains out of scope per the rules of engagement.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
REQUEST (Fictional / Synthetic)
POST /api/v1/webhooks/validate HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-ORGMANAGER-3100]
Content-Type: application/json

{ "callback_url": "https://observer.example.test/callback/123" }
```

```
RESPONSE (Fictional / Synthetic)
```

```
HTTP/1.1 200 OK
Content-Type: application/json

{ "reachable": true, "latency_ms": 142 }

(Observer endpoint log — fictional)
INBOUND: GET /callback/123  Source: NorthStar-Portal-Validator/1.0
```

Expected: The validation feature should resolve and restrict outbound destinations to public, non-internal hosts, and should never be usable to reach link-local or private-IP-range addresses.

Observed: The fictional server made an outbound request to the supplied attacker-controlled test endpoint with no destination restriction observed for the tested case.

Impact: In a real deployment, this pattern could potentially be abused to probe internal network ranges or cloud metadata endpoints; this assessment did not attempt or demonstrate access to any internal or metadata address, consistent with the non-destructive testing rules of engagement.

TMG-WAPT-006 — Privilege Escalation from Standard User to Organization Manager	**HIGH**
CVSS-Style Score: 7.6 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-269 — Improper Privilege Management**
Affected Area	Role Management
Affected Endpoint / Feature	*PATCH /api/v1/organizations/{orgId}/members/{userId}/role*
Description	The member-role-update endpoint checks that the requesting user is authenticated and belongs to the organization, but does not additionally verify that the requester's own role is authorized to grant the requested target role.
Business Context	Role assignment is a privileged administrative action; a Standard User granting themselves or another member the Organization Manager role bypasses the intended approval chain.
Security & Technical Impact	Security Impact: a fictional Standard User account successfully updated its own role to Organization Manager. Technical Impact: role-change authorization is enforced only at the organization-membership level, not the requester's-own-role level.
Attack Prerequisites	An authenticated Standard User session within the target organization.
Safe Proof of Concept (Summary)	*Illustrative role-update request submitted by a Standard User targeting their own membership record, successfully elevating to Organization Manager in the fictional test environment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-008 (redacted request/response, before/after role-state capture)*
Expected Behavior	Role-update requests should be authorized based on the requester's current role and should reject any role-change request targeting the requester's own account.
Observed (Fictional) Behavior	No requester-role authorization check was applied.
Root Cause	Missing function-level access control on a privileged administrative action.
Recommendation	Add explicit requester-role authorization to the role-update handler, and disallow self-targeted role changes entirely; log all role-change events for audit review.
Management Response	*Accepted; fictional identity-platform team will add requester-role validation and self-elevation blocking.*
Owner / Priority / Target / Status	**Identity & Access Lead (Fictional Role)** | 0-30 Days | 24 October 2026 | **Remediation In Progress**
Retest Recommendation	*Retest role-management endpoints across all six defined roles to confirm correct requester-role enforcement in both directions.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
REQUEST (Fictional / Synthetic)
PATCH /api/v1/organizations/ORG-1001/members/USER-5501/role HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-USER-5501]
Content-Type: application/json

{ "role": "organization_manager" }
```

```
RESPONSE (Fictional / Synthetic)
HTTP/1.1 200 OK
Content-Type: application/json
```

```
{ "user_id": "USER-5501", "role": "organization_manager", "updated": true }
```

Expected: Only an existing Organization Manager or Administrator should be authorized to change a member's role, and a user should never be able to elevate their own role.

Observed: The fictional endpoint accepted the self-elevation request without a requester-role authorization check.

Impact: Full vertical privilege escalation within the affected fictional organization, exposing organization-management, billing, and member-management functions to a former low-privilege user.

TMG-WAPT-007 — Excessive API Data Exposure Through Organization Endpoint	**HIGH**
CVSS-Style Score: 7.3 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-213 — Exposure of Sensitive Information Due to Incomplete Cleanup (Excessive Data Exposure)**
Affected Area	API — Organization Members
Affected Endpoint / Feature	*GET /api/v1/organizations/{orgId}/members*
Description	The organization-members listing endpoint returns full internal member objects — including fields intended only for administrative or billing contexts — to any authenticated member regardless of role, relying on the front-end to selectively display fields.
Business Context	Standard Users should see only a limited member directory (name, role, status); billing identifiers and internal audit fields are intended for Organization Manager and Administrator roles.
Security & Technical Impact	Security Impact: a fictional Standard User's API response included billing-linkage identifiers and internal risk-scoring metadata not shown in that role's UI. Technical Impact: field-level authorization (excessive data exposure, API3:2023-style) is enforced client-side only; the API contract itself returns the full internal object graph.
Attack Prerequisites	Any authenticated session able to call the members-listing endpoint directly (bypassing the UI).
Safe Proof of Concept (Summary)	*Illustrative response comparison showing UI-rendered fields versus the full fictional API payload returned to a Standard User session. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-009 (redacted response payload comparison by role)*
Expected Behavior	Field-level, role-aware serialization applied server-side for every response object.
Observed (Fictional) Behavior	Uniform full-object serialization regardless of requester role.
Root Cause	Absence of a server-side response-serialization layer that enforces field-level authorization by role.
Recommendation	Introduce role-aware DTO/serialization layer for all member- and organization-scoped endpoints; audit remaining API responses for similar excessive-exposure patterns.
Management Response	*Accepted; fictional API platform team will implement role-scoped serializers across the organization and members API surface.*
Owner / Priority / Target / Status	**API Platform Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | Open
Retest Recommendation	*Retest all organization- and member-scoped endpoints across each of the six defined roles to confirm field-level scoping.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

```
REQUEST (Fictional / Synthetic)
GET /api/v1/organizations/ORG-1001/members HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-USER-5501]
```

```
RESPONSE (Fictional / Synthetic)
HTTP/1.1 200 OK
Content-Type: application/json

[{
  "user_id": "USER-5502",
  "name": "Fictional Member Two",
  "role": "billing_user",
  "billing_account_ref": "BILL-REF-88213",
  "internal_risk_score": 12,
  "last_admin_note": "Fictional internal note — not intended for member view"
}]
```

Expected: The API should return a role-scoped field set matching what the requesting user is authorized to see, independent of front-end rendering.

Observed: All internal fields were present in the raw fictional API response regardless of requester role.

Impact: Exposure of internal billing linkage and internal-note metadata to unauthorized roles within the same organization.

TMG-WAPT-008 — File Download Authorization Bypass	**HIGH**
CVSS-Style Score: 7.1 (High) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-862 — Missing Authorization**
Affected Area	File Management
Affected Endpoint / Feature	*GET /api/v1/files/{fileId}/download*
Description	The file-download endpoint issues a signed object-storage URL based solely on a valid file ID, without confirming that the requesting user's organization owns the referenced file.
Business Context	Files uploaded through support tickets and invoices may include sensitive fictional attachments scoped to a single organization.
Security & Technical Impact	Security Impact: a fictional file ID belonging to Test Tenant A was downloadable using a session authenticated to Test Tenant B. Technical Impact: the download handler validates file-ID existence but not file-to-organization ownership against the requester's session.
Attack Prerequisites	A valid authenticated session and a known or enumerable file identifier belonging to another tenant.
Safe Proof of Concept (Summary)	*Illustrative cross-tenant file download using a sequential fictional file ID. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-010 (redacted request/response, ownership-mismatch confirmation)*
Expected Behavior	Ownership check enforced server-side prior to signed-URL issuance.
Observed (Fictional) Behavior	No ownership check performed; only file-ID existence was validated.
Root Cause	Missing object-level authorization on the download-URL issuance path, structurally similar to TMG-WAPT-001.
Recommendation	Add a mandatory ownership check (file-to-organization) before signed-URL issuance across all file-serving endpoints.
Management Response	*Accepted; fictional storage-platform team will add ownership verification to the download-handler.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest file-download and file-listing endpoints for ownership enforcement across all fictional test tenants.*

FULL EVIDENCE PANEL — ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE

REQUEST (Fictional / Synthetic)

```
GET /api/v1/files/FILE-90441/download HTTP/1.1
Host: portal.northstar-example.com
Authorization: Bearer [FICTIONAL-TOKEN-TESTUSER-1001]
```

RESPONSE (Fictional / Synthetic)

```
HTTP/1.1 302 Found
Location: https://storage.northstar-example.test/objects/FILE-90441?sig=[FICTIONAL-SIGNED-URL]
```

Expected: The handler should verify the file's owning organization matches the requester's organization before issuing any signed download URL.

Observed: A signed URL was issued for a fictional file owned by a different tenant.

Impact: Cross-tenant fictional document disclosure risk.

36 MEDIUM FINDINGS

The following 9 fictional Medium-severity findings reflect defense-in-depth gaps recommended for remediation within the 31-60 day window of the illustrative roadmap (Section 42).

TMG-WAPT-009 — Insufficient Rate Limiting on Password Reset Endpoint	MEDIUM
CVSS-Style Score: 5.9 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-307 — Improper Restriction of Excessive Authentication Attempts**
Affected Area	Account Recovery
Affected Endpoint / Feature	*POST /api/v1/account/password-reset/request*
Description	The password-reset-request endpoint permits a high fictional volume of requests for the same account within a short window before any throttling was observed.
Business Context	Password-reset request volume is a common target for enumeration and resource-exhaustion abuse.
Security & Technical Impact	Security & Technical Impact: in the fictional test environment, 50 sequential reset requests for the same test account completed without a rate-limit response; only email-delivery-provider-side batching was observed as an incidental control.
Attack Prerequisites	Network access to the public password-reset endpoint; no authentication required.
Safe Proof of Concept (Summary)	*A controlled, fictional burst of 50 password-reset requests against a single test account completed without an application-level rate-limit response. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-011 (fictional request-count/response-code table)*
Expected Behavior	Application-level rate limiting (e.g., per-account and per-source-IP) should trigger well before 50 requests.
Observed (Fictional) Behavior	No application-level throttling response was observed within the tested fictional volume.
Root Cause	Rate limiting for this endpoint is not implemented at the application layer.
Recommendation	Implement per-account and per-IP rate limiting with exponential backoff on the password-reset-request endpoint, consistent with controls already observed on the login endpoint (Section 45).
Management Response	*Accepted; fictional identity-platform team will extend existing login rate-limiting middleware to the password-reset endpoint.*
Owner / Priority / Target / Status	**Identity & Access Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | Remediation Planned
Retest Recommendation	*Retest with controlled fictional request volumes to confirm throttling activates at an appropriate threshold.*

TMG-WAPT-010 — JWT / Session Revocation Weakness	MEDIUM
CVSS-Style Score: 6.3 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-613 — Insufficient Session Expiration**
Affected Area	Session Management
Affected Endpoint / Feature	*POST /api/v1/auth/logout*
Description	Logout invalidates the refresh token but the short-lived access token issued to the client remains fictionally valid until its natural expiry, rather than being actively revoked.
Business Context	Users reasonably expect logout to immediately end their session on a given device, particularly on shared or lost devices.
Security & Technical Impact	Security & Technical Impact: a fictional access token captured before logout remained usable against protected endpoints for the remainder of its ~15-minute fictional lifetime after logout.
Attack Prerequisites	Possession of a still-valid access token from before the legitimate user's logout event.
Safe Proof of Concept (Summary)	*A fictional access token remained accepted by protected endpoints for a short window following an explicit logout call. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-012 (fictional token-lifetime timeline)*
Expected Behavior	Logout should revoke or blacklist the current access token (e.g., via a short server-side revocation check) in addition to the refresh token.
Observed (Fictional) Behavior	Only the refresh token was invalidated; the access token remained valid until natural expiry.
Root Cause	The JWT architecture relies on statelessness for the access token with no revocation-list check.
Recommendation	Introduce a lightweight server-side revocation check (e.g., short-TTL denylist) for access tokens on logout, or reduce

	access-token lifetime further to shrink the exposure window.
Management Response	*Accepted as a defense-in-depth improvement; fictional platform team will evaluate a revocation-list approach.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest logout behavior and confirm access-token rejection immediately following logout.*

TMG-WAPT-011 — CORS Trusts Unnecessary Origins	**MEDIUM**
CVSS-Style Score: 5.4 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-942 — Permissive Cross-domain Policy with Untrusted Domains**
Affected Area	Browser Security / CORS Configuration
Affected Endpoint / Feature	*All /api/v1/* endpoints*
Description	The API's CORS configuration reflects the request's Origin header for a broader set of fictional subdomains than the application actually uses, including several fictional preview/staging patterns.
Business Context	An overly broad CORS allow-list increases the number of origins from which authenticated cross-origin requests could be attempted if any of those origins were ever compromised or repurposed.
Security & Technical Impact	Security & Technical Impact: the fictional API reflected `Access-Control-Allow-Origin` for a wildcard-pattern staging domain not currently in active use, with `Access-Control-Allow-Credentials: true` also set.
Attack Prerequisites	Control of, or ability to serve content from, one of the overly broad allow-listed fictional origin patterns.
Safe Proof of Concept (Summary)	*A fictional cross-origin request from a stale staging-pattern origin received a permissive CORS response including credentialed-request support. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-013 (fictional CORS response header capture)*
Expected Behavior	CORS allow-list should be a minimal, explicit set of current production front-end origins.
Observed (Fictional) Behavior	A broader wildcard-pattern allow-list was in effect, including unused staging patterns.
Root Cause	CORS configuration was not pruned as staging/preview environments were decommissioned.
Recommendation	Reduce the CORS allow-list to the minimal explicit set of active origins and remove wildcard pattern-matching for credentialed requests.
Management Response	*Accepted; fictional platform team will audit and tighten the CORS configuration.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Remediation Planned**
Retest Recommendation	*Retest CORS response headers against the pruned allow-list from a range of fictional test origins.*

TMG-WAPT-012 — Verbose Error Messages Reveal Internal Application Details	**MEDIUM**
CVSS-Style Score: 5.3 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-209 — Generation of Error Message Containing Sensitive Information**
Affected Area	Error Handling
Affected Endpoint / Feature	*Multiple /api/v1/* endpoints (malformed-input cases)*
Description	Several fictional API endpoints return raw exception detail — including internal file paths and ORM query fragments — when supplied with malformed input, rather than a generic error response.
Business Context	Verbose error output is a common reconnaissance aid, revealing framework, library, and internal-structure details useful to an attacker profiling the application.
Security & Technical Impact	Security & Technical Impact: fictional malformed-input test cases against several endpoints returned stack-trace fragments referencing internal fictional module paths.
Attack Prerequisites	Ability to submit malformed input to an affected endpoint; no authentication required for some affected endpoints.
Safe Proof of Concept (Summary)	*Fictional malformed-JSON submissions returned raw internal exception detail instead of a generic error envelope. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-014 (fictional redacted error-response samples)*
Expected Behavior	A generic, consistent error envelope should be returned to clients, with detailed diagnostics logged server-side only.
Observed (Fictional) Behavior	Raw exception detail was returned directly in several fictional API responses.
Root Cause	Inconsistent centralized error-handling middleware coverage across the API surface.
Recommendation	Standardize a centralized error-handling middleware that returns a generic client-facing error envelope for all unhandled

	exceptions, with full detail retained only in server-side logs.
Management Response	*Accepted; fictional platform team will extend centralized error handling to the remaining endpoints.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest malformed-input handling across the full fictional endpoint inventory.*

TMG-WAPT-013 — Missing Security Header Defense	**MEDIUM**
CVSS-Style Score: 5.0 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-693 — Protection Mechanism Failure**
Affected Area	Browser Security / Response Headers
Affected Endpoint / Feature	*All application front-end responses*
Description	The fictional application does not set a Content-Security-Policy header, and X-Frame-Options / frame-ancestors protection is inconsistently applied across pages.
Business Context	Security response headers are a defense-in-depth layer that reduces the impact of any future front-end injection issue and provides clickjacking protection.
Security & Technical Impact	Security & Technical Impact: fictional response-header capture across representative pages showed no CSP and inconsistent frame-protection headers.
Attack Prerequisites	N/A — a configuration observation rather than an independently exploitable condition.
Safe Proof of Concept (Summary)	*Fictional header capture across representative pages confirmed the absence of a CSP and inconsistent frame-protection coverage. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-015 (fictional response-header matrix)*
Expected Behavior	A consistent CSP, X-Frame-Options/frame-ancestors, and related headers applied platform-wide.
Observed (Fictional) Behavior	Headers were inconsistently applied and CSP was absent across all tested fictional pages.
Root Cause	No centralized security-header middleware is applied uniformly across the front-end.
Recommendation	Introduce a centralized security-header middleware (CSP, X-Frame-Options/frame-ancestors, X-Content-Type-Options, HSTS, Referrer-Policy) applied to every response.
Management Response	*Accepted; fictional front-end platform team will roll out a shared security-header baseline.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Remediation Planned**
Retest Recommendation	*Retest header presence and correctness across all major application routes.*

TMG-WAPT-014 — Mass Assignment in Organization Profile Update	**MEDIUM**
CVSS-Style Score: 6.1 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-915 — Improperly Controlled Modification of Dynamically-Determined Object Attributes**
Affected Area	Organization Management
Affected Endpoint / Feature	*PATCH /api/v1/organizations/{orgId}/profile*
Description	The organization-profile update endpoint binds the full request body to the underlying data model, allowing fields not exposed in the UI (such as an internal risk-tier flag) to be modified if included in the request.
Business Context	Internal-only fields such as risk classification are intended to be set exclusively by internal review processes, not by customer-facing update calls.
Security & Technical Impact	Security & Technical Impact: a fictional test request including an undocumented `risk_tier` field successfully modified that internal value alongside the legitimate profile fields.
Attack Prerequisites	An authenticated Organization Manager session with legitimate access to the profile-update endpoint.
Safe Proof of Concept (Summary)	*A fictional profile-update request containing an additional undocumented field was accepted and applied. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-016 (fictional before/after object-state comparison)*
Expected Behavior	The update handler should bind only an explicit allow-list of client-editable fields to the underlying model.
Observed (Fictional) Behavior	The handler bound the entire request body, including non-exposed internal fields.
Root Cause	Use of a generic object-binding pattern without an explicit field allow-list on a privileged data model.
Recommendation	Replace generic body-binding with an explicit allow-listed update DTO for every write endpoint that touches an object

	containing internal-only fields.
Management Response	*Accepted; fictional API platform team will introduce allow-listed update DTOs across write endpoints.*
Owner / Priority / Target / Status	**API Platform Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest all profile/object update endpoints for mass-assignment exposure of internal-only fields.*

TMG-WAPT-015 — Webhook Replay Protection Missing	**MEDIUM**
CVSS-Style Score: 5.7 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-345 — Insufficient Verification of Data Authenticity**
Affected Area	Webhook Security
Affected Endpoint / Feature	*POST (customer-hosted webhook receiver, outbound event delivery)*
Description	Outbound webhook event payloads are signed, but the signature does not incorporate a timestamp or nonce, and the fictional receiver reference implementation does not reject a captured-and-resent (replayed) event.
Business Context	Customers build automation on webhook events; a replayed event could cause duplicate downstream processing (e.g., duplicate order-fulfillment triggers) if the customer's own receiver does not independently de-duplicate.
Security & Technical Impact	Security & Technical Impact: a fictional captured webhook payload, when resent unmodified, passed signature validation a second time because the signature covers only the payload body, not a timestamp or nonce.
Attack Prerequisites	Ability to capture a legitimate previously-delivered webhook payload (e.g., from a compromised or misconfigured receiver endpoint in the fictional scenario).
Safe Proof of Concept (Summary)	*A captured fictional webhook payload replayed unmodified passed signature validation on resend. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-017 (fictional signature-validation replay test)*
Expected Behavior	Signatures should incorporate a timestamp/nonce, with the platform documenting a recommended freshness window and duplicate-event-ID check for receivers.
Observed (Fictional) Behavior	Signature validation covered payload content only, with no timestamp or nonce component.
Root Cause	Webhook signing scheme does not include replay-protection elements.
Recommendation	Add a timestamp and nonce (or monotonic event ID) to the signed payload envelope, document a freshness-window check, and provide a reference receiver implementation demonstrating replay rejection.
Management Response	*Accepted; fictional integrations team will update the webhook signing scheme and reference documentation.*
Owner / Priority / Target / Status	**Integrations Platform Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Remediation Planned**
Retest Recommendation	*Retest webhook signature validation for replay rejection after the timestamp/nonce scheme is introduced.*

TMG-WAPT-016 — Insufficient File Validation	**MEDIUM**
CVSS-Style Score: 5.6 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-434 — Unrestricted Upload of File with Dangerous Type**
Affected Area	File Upload
Affected Endpoint / Feature	*POST /api/v1/files/upload*
Description	File-type validation on upload relies on the client-supplied filename extension and MIME-type header rather than server-side content inspection.
Business Context	Uploaded files (support attachments, invoice documents) are later served back to users; insufficiently validated file types increase downstream content-handling risk.
Security & Technical Impact	Security & Technical Impact: a fictional test file with a mismatched extension/content-type pairing was accepted by the upload handler in the test environment.
Attack Prerequisites	An authenticated session able to reach the file-upload endpoint.
Safe Proof of Concept (Summary)	*A fictional test file with a deliberately mismatched extension and declared MIME type was accepted without a content-based validation failure. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-018 (fictional upload-acceptance test log)*
Expected Behavior	Server-side content inspection (e.g., magic-byte/signature validation) should confirm the actual file type independent of client-supplied metadata.
Observed (Fictional) Behavior	Validation relied on client-supplied extension/MIME-type only.
Root Cause	Missing server-side content-type verification step in the upload pipeline.

Recommendation	Add server-side file-signature (magic-byte) validation and route uploaded files through the existing inspection workflow referenced in Section 45 (Positive Controls) before making them retrievable.
Management Response	*Accepted; fictional platform team will add content-based validation to the upload pipeline.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest upload validation with a range of fictional mismatched-type test files.*

TMG-WAPT-017 — Business Logic Replay in Discount Workflow	**MEDIUM**
CVSS-Style Score: 5.8 (Medium) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-841 — Improper Enforcement of Behavioral Workflow**
Affected Area	Billing / Discount Redemption
Affected Endpoint / Feature	*POST /api/v1/billing/discounts/redeem*
Description	A single-use discount code was, in the fictional test environment, capable of being redeemed a second time on the same test organization when the redemption request was resent shortly after the first, due to a narrow validation window.
Business Context	Single-use promotional discounts are relied upon for controlled revenue-impact promotions; repeat redemption undermines that control.
Security & Technical Impact	Security & Technical Impact: two rapidly-sequential fictional redemption requests for the same single-use code both returned success in the test environment, applying the discount twice.
Attack Prerequisites	An authenticated Billing User session and the ability to submit two redemption requests in rapid succession (related to, but distinct from, the race-condition class described in Section 31).
Safe Proof of Concept (Summary)	*Two fictional rapid-sequence redemption requests for the same single-use code both succeeded in the test environment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-019 (fictional redemption-count/state log)*
Expected Behavior	Redemption state should be checked and updated atomically so a second concurrent or rapid-sequence request for the same code is rejected.
Observed (Fictional) Behavior	A narrow window between the validity check and the state update allowed a second success in the fictional test.
Root Cause	Non-atomic check-then-update pattern in the discount-redemption handler.
Recommendation	Enforce atomic, database-level uniqueness/locking on redemption-state updates for single-use codes.
Management Response	*Accepted; fictional billing-platform team will introduce an atomic redemption-state transition.*
Owner / Priority / Target / Status	**Director, Billing Platform (Fictional Role)** | 31-60 Days | 23 November 2026 | **Open**
Retest Recommendation	*Retest with controlled concurrent-request scenarios to confirm single-use enforcement.*

37 LOW FINDINGS

The following 7 fictional Low-severity findings are hardening opportunities recommended for the 61-90 day window of the illustrative roadmap.

TMG-WAPT-018 — Technology Version Disclosure	LOW
CVSS-Style Score: 3.1 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-200 — Exposure of Sensitive Information to an Unauthorized Actor**
Affected Area	Server Configuration
Affected Endpoint / Feature	*All application responses (Server / X-Powered-By headers)*
Description	Fictional response headers disclosed the specific backend framework version in use.
Business Context	Version disclosure narrows the search space for an attacker researching known issues in a specific framework version.
Security & Technical Impact	Security & Technical Impact: fictional header capture showed a specific framework version string on every response.
Safe Proof of Concept (Summary)	*Fictional header capture across sampled endpoints consistently disclosed backend framework version. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-020 (fictional header sample)*
Expected Behavior	Version-identifying headers suppressed or genericized in production responses.
Observed (Fictional) Behavior	Version string present on all sampled fictional responses.
Root Cause	Default framework configuration was not hardened to suppress version headers.
Recommendation	Disable or genericize version-disclosing headers at the framework/edge layer.
Management Response	*Accepted as a hardening item for the defense-in-depth backlog.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm header suppression on retest.*

TMG-WAPT-019 — Verbose Validation Response	LOW
CVSS-Style Score: 2.9 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-209 — Generation of Error Message Containing Sensitive Information**
Affected Area	Registration / Input Validation
Affected Endpoint / Feature	*POST /api/v1/auth/register*
Description	Field-level validation responses on registration distinguish between "invalid format" and "email already registered," providing a mild account-enumeration signal.
Business Context	Related to, but lower-severity than, the account-enumeration considerations covered in Section 12; distinguishable validation messages remain a minor information-disclosure vector.
Security & Technical Impact	Security & Technical Impact: fictional registration attempts with a known-registered test email returned a distinguishable message from attempts with a malformed email.
Safe Proof of Concept (Summary)	*Fictional side-by-side comparison of validation messages for a malformed versus an already-registered test email. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-021 (fictional response-message comparison)*
Expected Behavior	Generic validation messaging that does not distinguish existence from format issues.
Observed (Fictional) Behavior	Distinguishable messaging was present.
Root Cause	Validation-message design prioritized user experience over enumeration resistance.
Recommendation	Adopt generic validation messaging consistent with the enumeration-resistant pattern already used on the login endpoint.
Management Response	*Accepted as a minor hardening item.*
Owner / Priority / Target / Status	**Identity & Access Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm generic messaging on retest.*

TMG-WAPT-020 — Missing Referrer-Policy Hardening	LOW
CVSS-Style Score: 2.6 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-693 — Protection Mechanism Failure**
Affected Area	Browser Security / Response Headers
Affected Endpoint / Feature	*All application front-end responses*
Description	No explicit Referrer-Policy header was observed, leaving the browser default in effect across the fictional application.
Business Context	An explicit, stricter Referrer-Policy reduces incidental leakage of full URLs (which may contain query parameters) to third-party destinations via the Referer header.
Security & Technical Impact	Security & Technical Impact: fictional header capture showed no explicit Referrer-Policy value set.
Safe Proof of Concept (Summary)	*Fictional header capture confirmed the header was absent across sampled pages. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-022 (fictional header sample)*
Expected Behavior	An explicit `strict-origin-when-cross-origin` or stricter Referrer-Policy applied platform-wide.
Observed (Fictional) Behavior	No explicit policy set; browser default in effect.
Root Cause	Not yet included in the centralized header baseline referenced in TMG-WAPT-013.
Recommendation	Include Referrer-Policy in the centralized security-header rollout planned for TMG-WAPT-013.
Management Response	*Accepted; will be bundled with the TMG-WAPT-013 header rollout.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Remediation Planned**
Retest Recommendation	*Confirm header presence alongside the TMG-WAPT-013 retest.*

TMG-WAPT-021 — Unnecessary Client-Side Debug Logging	LOW
CVSS-Style Score: 2.8 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-532 — Insertion of Sensitive Information into Log File**
Affected Area	Client-Side Security
Affected Endpoint / Feature	*Front-end application bundle (browser console output)*
Description	The fictional production front-end bundle retains verbose `console.log` debug statements, including non-sensitive internal state objects, that were disabled in most but not all modules.
Business Context	Debug logging left enabled in production increases the front-end's information footprint and can occasionally evolve to include sensitive data if not consistently reviewed.
Security & Technical Impact	Security & Technical Impact: fictional browser console output during testing included internal component-state logging on a subset of pages; no credentials or tokens were observed in this fictional sample.
Safe Proof of Concept (Summary)	*Fictional browser console capture showed residual debug logging on a subset of application pages. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-023 (fictional console-output sample)*
Expected Behavior	Debug logging stripped from production builds via the CI/CD build pipeline.
Observed (Fictional) Behavior	Debug logging present on a subset of pages, inconsistently stripped.
Root Cause	Build-time log-stripping configuration is not uniformly applied across all front-end modules.
Recommendation	Extend the existing build-time log-stripping step to cover all modules; add a CI check to fail the build on residual debug logging.
Management Response	*Accepted as a hardening item for the front-end build pipeline.*
Owner / Priority / Target / Status	**Front-End Engineering Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm log-stripping coverage across all modules on retest.*

TMG-WAPT-022 — Logout Does Not Immediately Clear One Non-Privileged Local Session Artifact	LOW

CVSS-Style Score: 2.5 (Low) — Illustrative CVSS v3.1-inspired score	CWE: CWE-613 — Insufficient Session Expiration
Affected Area	Client-Side Session Handling
Affected Endpoint / Feature	*Front-end logout handler*
Description	Logout clears the primary authentication tokens but leaves one non-privileged UI-preference artifact (a cached "last viewed organization" value) in browser local storage.
Business Context	The retained artifact does not grant access on its own, but represents an inconsistency in the logout "clean state" behavior worth correcting for defense-in-depth.
Security & Technical Impact	Security & Technical Impact: fictional local-storage inspection after logout showed the non-privileged preference value still present; no authentication material remained.
Safe Proof of Concept (Summary)	*Fictional local-storage inspection after logout confirmed only a non-privileged UI-preference value remained. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-024 (fictional local-storage state capture, before/after logout)*
Expected Behavior	Logout should clear all application-related local-storage entries, not only authentication tokens.
Observed (Fictional) Behavior	One non-privileged preference value persisted after logout.
Root Cause	The logout handler's storage-clearing routine targets an explicit key list that does not include the newer preference key.
Recommendation	Update the logout handler to clear the full application storage namespace rather than an explicit key list.
Management Response	*Accepted as a minor hardening item.*
Owner / Priority / Target / Status	**Front-End Engineering Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm full storage-namespace clearing on retest.*

TMG-WAPT-023 — Password Policy Documentation Inconsistency	LOW
CVSS-Style Score: 2.2 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: N/A — Documentation / Process Observation**
Affected Area	Account Management
Affected Endpoint / Feature	*Registration / password-change user-facing help text*
Description	The fictional password-complexity help text shown to users during registration understates the actual enforced minimum length by two characters.
Business Context	A minor documentation mismatch rather than a technical control gap; the enforced control itself was validated as adequate during authentication testing (Section 12).
Security & Technical Impact	Security & Technical Impact: no security control weakness — this is a user-facing documentation inconsistency identified during authentication testing.
Safe Proof of Concept (Summary)	*Fictional side-by-side comparison of displayed help text versus enforced server-side minimum length. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-025 (fictional help-text/enforcement comparison)*
Expected Behavior	Displayed policy text should match the enforced server-side policy exactly.
Observed (Fictional) Behavior	Displayed text understated the enforced minimum length.
Root Cause	Help text was not updated when the server-side policy was last strengthened.
Recommendation	Update the user-facing help text to match the current enforced password policy.
Management Response	*Accepted; a documentation-only fix.*
Owner / Priority / Target / Status	**Front-End Engineering Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm text/enforcement alignment on retest.*

TMG-WAPT-024 — Security Configuration Hardening Opportunity	LOW
CVSS-Style Score: 3.0 (Low) — Illustrative CVSS v3.1-inspired score	**CWE: CWE-16 — Configuration**
Affected Area	Security Configuration

Affected Endpoint / Feature	*Application-wide HTTP method handling*
Description	Several fictional endpoints accept the `TRACE` and `OPTIONS` HTTP methods without an explicit, deliberate handler, returning default framework behavior rather than a defined response.
Business Context	Unused HTTP methods left in their framework-default state are a minor attack-surface and configuration-hygiene item.
Security & Technical Impact	Security & Technical Impact: fictional method-enumeration testing found `TRACE` enabled on a subset of sampled endpoints with default framework behavior.
Safe Proof of Concept (Summary)	*Fictional HTTP method enumeration found TRACE enabled by default on a subset of endpoints. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-026 (fictional method-enumeration table)*
Expected Behavior	Unused HTTP methods explicitly disabled at the edge/WAF or application layer.
Observed (Fictional) Behavior	Default framework behavior in effect for unused methods on a subset of endpoints.
Root Cause	No explicit method allow-list configured at the edge layer.
Recommendation	Configure an explicit HTTP method allow-list at the CDN/WAF edge layer, disabling TRACE and unused methods platform-wide.
Management Response	*Accepted as a hardening item for the edge configuration backlog.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | 61-90 Days | 08 December 2026 | **Open**
Retest Recommendation	*Confirm method allow-list enforcement on retest.*

38 INFORMATIONAL FINDINGS

The following 8 fictional Informational observations carry no direct exploitation path and are recommended for the ongoing defense-in-depth backlog.

TMG-WAPT-025 — Security.txt Not Present	INFORMATIONAL
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	CWE: N/A
Affected Area	Vulnerability Disclosure Process
Affected Endpoint / Feature	*/.well-known/security.txt*
Description	The fictional application does not publish a security.txt file describing a coordinated vulnerability-disclosure contact and process.
Business Context	A published security.txt is a low-cost best practice that streamlines external researcher reporting.
Security & Technical Impact	Observation only — no technical control gap.
Safe Proof of Concept (Summary)	*Fictional request to /.well-known/security.txt returned 404. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-027 (fictional request/response)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	File not present in the fictional test environment.
Root Cause	Not yet implemented.
Recommendation	Publish a security.txt file per the informal community convention, pointing to the existing security@tmgsec.com-style fictional reporting contact appropriate for NorthStar.
Management Response	*Accepted as a low-effort improvement for a future release.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; confirm on next general assessment.*

TMG-WAPT-026 — API Documentation Exposure — Intended but Reviewable	INFORMATIONAL
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	CWE: N/A
Affected Area	API Documentation
Affected Endpoint / Feature	*/api/v1/docs*
Description	Interactive API documentation is publicly reachable without authentication; this appears to be an intended developer-experience feature but is noted for periodic review to confirm no sensitive internal-only endpoints are described there.
Business Context	Public API documentation is a common and often intentional practice; the observation is limited to recommending periodic content review.
Security & Technical Impact	Observation only — reviewed documentation content did not disclose any fictional internal-only endpoint in this sample.
Safe Proof of Concept (Summary)	*Fictional documentation endpoint reachable without authentication; content reviewed and found consistent with public API surface. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-028 (fictional documentation content review notes)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Publicly reachable, content consistent with intended public API surface.
Root Cause	N/A.
Recommendation	Maintain a periodic review process to ensure internal-only endpoints are never included in the public documentation set.
Management Response	*Accepted; will be folded into the existing documentation review cadence.*
Owner / Priority / Target / Status	**API Platform Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; confirm on next general assessment.*

TMG-WAPT-027 — Detailed Technology Fingerprinting	INFORMATIONAL
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: CWE-200**
Affected Area	Reconnaissance Surface
Affected Endpoint / Feature	*Multiple*
Description	Passive fictional fingerprinting (response headers, error signatures, asset bundling patterns) was sufficient to identify the general backend and front-end frameworks in use, consistent with TMG-WAPT-018.
Business Context	Framework fingerprinting is common for modern web applications and difficult to fully eliminate; noted here as a consolidated reconnaissance observation.
Security & Technical Impact	Observation only, related to TMG-WAPT-018.
Safe Proof of Concept (Summary)	*Fictional passive fingerprinting summary compiled during reconnaissance (Section 11). [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-029 (fictional fingerprinting summary)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Consistent with modern web-application fingerprinting exposure generally.
Root Cause	Inherent to the technology stack; not a discrete control gap.
Recommendation	No dedicated action beyond the header-suppression work already planned under TMG-WAPT-018.
Management Response	*Acknowledged; tracked jointly with TMG-WAPT-018.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; confirm on next general assessment.*

TMG-WAPT-028 — Unused Security Response Header Opportunity	INFORMATIONAL
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: CWE-693**
Affected Area	Browser Security / Response Headers
Affected Endpoint / Feature	*All application front-end responses*
Description	The `Permissions-Policy` header (restricting browser feature access such as geolocation/camera) is not set; the fictional application does not use these browser features, so the header would be a strict-improvement no-risk addition.
Business Context	Complements the broader header-hardening work already tracked under TMG-WAPT-013.
Security & Technical Impact	Observation only.
Safe Proof of Concept (Summary)	*Fictional header capture confirmed Permissions-Policy absence. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-030 (fictional header sample)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Header absent across sampled fictional pages.
Root Cause	Not yet included in the header baseline.
Recommendation	Bundle Permissions-Policy into the TMG-WAPT-013 header rollout.
Management Response	*Accepted; will be bundled with TMG-WAPT-013.*
Owner / Priority / Target / Status	**Platform Engineering Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; confirm alongside TMG-WAPT-013 retest.*

TMG-WAPT-029 — Exposed Non-Sensitive Build Metadata	INFORMATIONAL
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: CWE-200**
Affected Area	Front-End Build Artifacts

Affected Endpoint / Feature	*Front-end bundle metadata / source-map reference comments*
Description	The fictional front-end bundle includes a non-sensitive build-identifier comment (build hash and date) that is not itself sensitive but contributes marginally to fingerprinting.
Business Context	Low-impact observation; noted for completeness alongside the fingerprinting-related findings above.
Security & Technical Impact	Observation only.
Safe Proof of Concept (Summary)	*Fictional bundle inspection located a non-sensitive build-identifier comment. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-031 (fictional bundle excerpt)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Non-sensitive build metadata present in bundle comments.
Root Cause	Default build-tool behavior; not a discrete control gap.
Recommendation	Optional: strip build-identifier comments from production bundles as a minor hardening step.
Management Response	*Acknowledged; low priority.*
Owner / Priority / Target / Status	**Front-End Engineering Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure.*

TMG-WAPT-030 — Session Management Documentation Improvement	**INFORMATIONAL**
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: N/A**
Affected Area	Internal Documentation
Affected Endpoint / Feature	*N/A — process observation*
Description	Internal fictional engineering documentation describing session-lifetime and refresh-token-rotation behavior was found to be out of date relative to the current implementation observed during testing.
Business Context	Accurate internal documentation supports faster, safer incident response and onboarding.
Security & Technical Impact	Observation only — a process/documentation item, not a technical control gap.
Safe Proof of Concept (Summary)	*Fictional documentation review identified stale session-lifetime values compared to observed behavior. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-032 (fictional documentation excerpt vs. observed behavior)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Documentation described session lifetimes no longer matching current configuration.
Root Cause	Documentation not updated alongside the most recent session-configuration change.
Recommendation	Update internal session-management documentation to reflect current configuration values.
Management Response	*Accepted; documentation update scheduled.*
Owner / Priority / Target / Status	**Platform Security Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure.*

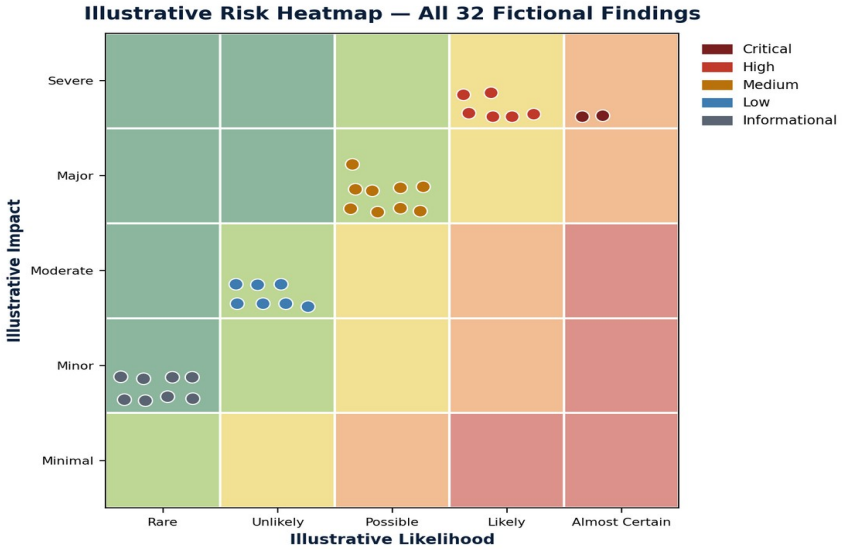
TMG-WAPT-031 — Security Monitoring Enhancement Opportunity	**INFORMATIONAL**
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: N/A**
Affected Area	Logging & Monitoring
Affected Endpoint / Feature	*N/A — process observation*
Description	Centralized security logging captures authentication and role-change events (a positive control, Section 45), but does not yet include a dedicated alert rule for the specific self-role-elevation pattern identified in TMG-WAPT-006.
Business Context	Monitoring enhancements complement the underlying control fix and support faster detection of similar patterns in the future.
Security & Technical Impact	Observation only; a recommended enhancement to already-solid logging coverage.

Safe Proof of Concept (Summary)	*Fictional review of alert-rule configuration found no dedicated rule for self-role-elevation attempts. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*EV-WAPT-033 (fictional alert-rule configuration review)*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Event is logged but not yet alerted on as a distinct high-signal pattern.
Root Cause	Alert-rule catalog has not yet been updated to reflect this assessment's findings.
Recommendation	Add a dedicated alert rule for self-targeted role-change attempts, informed by TMG-WAPT-006.
Management Response	*Accepted; will be added alongside the TMG-WAPT-006 remediation.*
Owner / Priority / Target / Status	**Security Operations Lead (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; confirm alongside TMG-WAPT-006 retest.*

TMG-WAPT-032 — Defense-in-Depth Recommendation for Sensitive Workflows	**INFORMATIONAL**
CVSS-Style Score: N/A — Informational observation, no CVSS score assigned	**CWE: N/A**
Affected Area	Cross-Cutting / Sensitive Workflow Design
Affected Endpoint / Feature	*N/A — design observation*
Description	Several sensitive workflows (role change, plan-tier change, email change) rely on a single authorization check rather than a layered pattern (e.g., step-up confirmation or secondary approval) for their highest-impact actions.
Business Context	This is a forward-looking architectural recommendation rather than a specific control failure, intended to reduce the blast radius of any single future authorization defect.
Security & Technical Impact	Observation only — a design-pattern recommendation spanning multiple sections of this fictional assessment.
Safe Proof of Concept (Summary)	*Cross-referenced design observation drawn from TMG-WAPT-001, 002, and 006. [ILLUSTRATIVE / FICTIONAL SAMPLE EVIDENCE]*
Evidence Reference	*Cross-reference: TMG-WAPT-001, TMG-WAPT-002, TMG-WAPT-006*
Expected Behavior	N/A — recommendation, not a control failure.
Observed (Fictional) Behavior	Single-check authorization pattern observed across several high-impact fictional workflows.
Root Cause	Architectural pattern choice rather than a specific implementation defect.
Recommendation	Consider a layered authorization pattern (step-up confirmation, secondary approval, or short-lived elevated-action tokens) for the platform's highest-impact workflows as a longer-term hardening investment.
Management Response	*Accepted as a longer-term architectural consideration for the fictional product roadmap.*
Owner / Priority / Target / Status	**VP Engineering (Fictional Role)** | Backlog — Defense-in-Depth | Backlog — Next Planning Cycle | **Open**
Retest Recommendation	*Not required for closure; revisit as part of the next full assessment cycle.*

39 RISK HEATMAP

The heatmap below plots all 32 fictional findings by illustrative likelihood and impact, reflecting the severity assigned to each finding in Sections 34-38. This view is intended to support prioritization discussions alongside the Management Action Plan (Section 43).

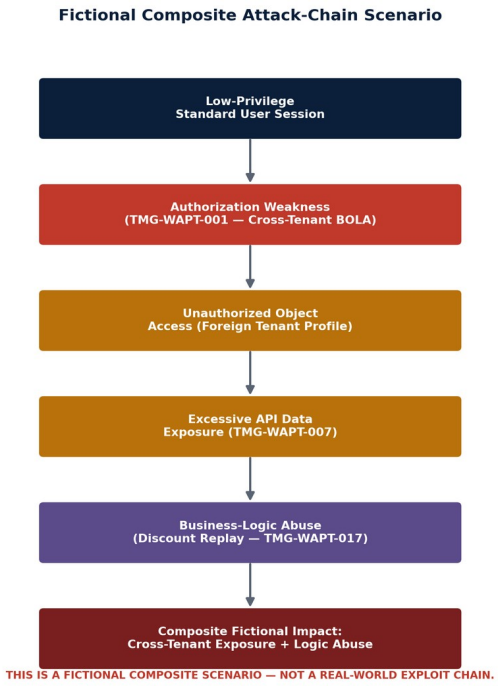


Illustrative risk heatmap — all 32 fictional findings plotted by likelihood and impact.

This heatmap reflects fictional, illustrative severity data only and does not represent the risk posture of any real organization.

40 ATTACK CHAIN ANALYSIS

Individual findings are often most meaningful in combination. This section presents one fictional composite attack-chain scenario, illustrating how several independently Medium-to-Critical findings from this assessment could combine into a more significant illustrative impact if left unaddressed together.



Fictional composite attack-chain scenario — not a real-world exploit chain.

Fictional Composite Scenario Narrative

Starting from a low-privilege, authenticated Standard User session, the fictional cross-tenant authorization weakness (TMG-WAPT-001) permits access to another organization's profile object. The excessive API data exposure finding (TMG-WAPT-007) means that object — and equivalent objects reachable the same way — returns more internal detail than intended. Independently, the business-logic replay weakness in the discount-redemption workflow (TMG-WAPT-017) shows that workflow-state enforcement has gaps elsewhere in the platform. Combined, an attacker following this fictional path could reach cross-tenant data exposure together with a business-logic abuse pattern — a composite illustrative impact more significant than any single finding in isolation.

THIS IS A FICTIONAL COMPOSITE ATTACK SCENARIO. It does not describe, and must not be construed as, an exploit chain against any real system.

41 BUSINESS IMPACT ANALYSIS

The table below maps each Critical and High fictional finding to the illustrative business dimensions it most directly affects, supporting prioritization conversations beyond pure technical severity.

Finding ID	Confidentiality	Integrity	Availability	Fraud / Revenue Risk	Customer Trust
TMG-WAPT-001	High	Low	None	Medium	High
TMG-WAPT-002	Low	High	None	High	Medium
TMG-WAPT-003	Medium	Medium	None	Low	Medium
TMG-WAPT-004	Medium	High	None	Medium	High
TMG-WAPT-005	Medium	Low	Low	Low	Medium
TMG-WAPT-006	High	High	None	Medium	High
TMG-WAPT-007	Medium	Low	None	Low	Medium
TMG-WAPT-008	Medium	Low	None	Low	Medium

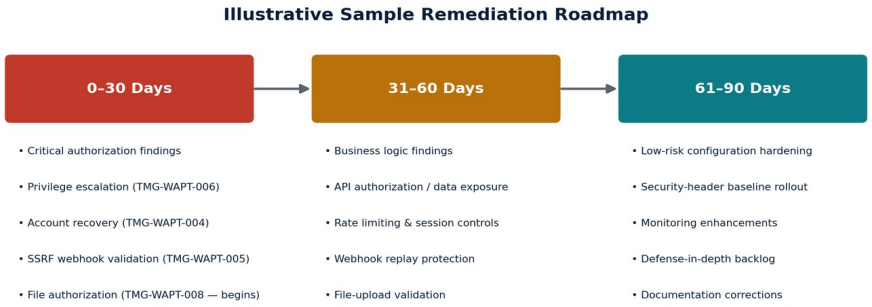
Illustrative Regulatory & Operational Risk Note

As a fictional digital-payments-adjacent platform, NorthStar's illustrative regulatory risk considerations would include data-protection and payment-industry expectations around access control and cardholder-adjacent data handling. This report does not

assess compliance with any specific regulatory framework; the fictional findings above are offered only as illustrative business-impact context.

42 REMEDIATION ROADMAP

The illustrative sample remediation roadmap below sequences all 32 fictional findings across three phases, prioritizing Critical and High authorization findings first.



ILLUSTRATIVE SAMPLE REMEDIATION ROADMAP — fictional sequencing and dates.

0-30 Days

- Critical authorization findings — TMG-WAPT-001, TMG-WAPT-002
- Privilege escalation — TMG-WAPT-006
- Account recovery — TMG-WAPT-004
- SSRF webhook validation — TMG-WAPT-005
- Stored XSS in support workflow — TMG-WAPT-003

31-60 Days

- Business logic findings — TMG-WAPT-017
- API authorization / data exposure — TMG-WAPT-007, TMG-WAPT-008, TMG-WAPT-014
- Rate limiting & session controls — TMG-WAPT-009, TMG-WAPT-010
- Webhook replay protection — TMG-WAPT-015
- File-upload validation — TMG-WAPT-016
- CORS and header hardening — TMG-WAPT-011, TMG-WAPT-012, TMG-WAPT-013

61-90 Days

- Low-risk configuration hardening — TMG-WAPT-018, TMG-WAPT-020, TMG-WAPT-023, TMG-WAPT-024
- Security-header baseline completion — TMG-WAPT-019, TMG-WAPT-021, TMG-WAPT-022
- Monitoring and documentation enhancements — TMG-WAPT-025 through TMG-WAPT-032

ILLUSTRATIVE SAMPLE REMEDIATION ROADMAP — sequencing, owners, and dates are fictional.

43 MANAGEMENT ACTION PLAN

The table below tracks the fictional management response, ownership, and validation approach for all 32 findings, ensuring every finding identified in Sections 34-38 appears here exactly once.

Finding ID	Owner	Priority	Target Date	Status	Validation Method	Remediation (Summary)
TMG-WAPT-001	VP Engineering	Immediate — 0-30 Days	10 October 2026	Remediation In Progress	Full or Targeted Retest	Enforce server-side tenant-scoping on every organization-sc…

Finding ID	Owner	Priority	Target Date	Status	Validation Method	Remediation (Summary)
TMG-WAPT-002	Director, Billing Platform	Immediate — 0-30 Days	10 October 2026	Remediation In Progress	Full or Targeted Retest	Remove client-controllable authorization fields from the re...
TMG-WAPT-003	Engineering Lead, Support...	0-30 Days	24 October 2026	Open	Full or Targeted Retest	Apply a single shared, context-aware output-encoding compon...
TMG-WAPT-004	Identity & Access Lead	0-30 Days	24 October 2026	Open	Full or Targeted Retest	Bind each confirmation code to its originating change-reque...
TMG-WAPT-005	Platform Security Lead	0-30 Days	24 October 2026	Remediation Planned	Full or Targeted Retest	Implement an egress allow-list and explicit blocklist for p...
TMG-WAPT-006	Identity & Access Lead	0-30 Days	24 October 2026	Remediation In Progress	Full or Targeted Retest	Add explicit requester-role authorization to the role-updat...
TMG-WAPT-007	API Platform Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Introduce role-aware DTO/serialization layer for all member...
TMG-WAPT-008	Platform Security Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Add a mandatory ownership check (file-to-organization) befo...
TMG-WAPT-009	Identity & Access Lead	31-60 Days	23 November 2026	Remediation Planned	Full or Targeted Retest	Implement per-account and per-IP rate limiting with exponen...
TMG-WAPT-010	Platform Security Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Introduce a lightweight server-side revocation check (e.g.,...
TMG-WAPT-011	Platform Security Lead	31-60 Days	23 November 2026	Remediation Planned	Full or Targeted Retest	Reduce the CORS allow-list to the minimal explicit set of a...
TMG-WAPT-012	Platform Engineering Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Standardize a centralized error-handling middleware that re...
TMG-WAPT-013	Platform Engineering Lead	31-60 Days	23 November 2026	Remediation Planned	Full or Targeted Retest	Introduce a centralized security-header middleware (CSP, X-...
TMG-WAPT-014	API Platform Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Replace generic body-binding with an explicit allow-listed...
TMG-WAPT-015	Integrations Platform Lead	31-60 Days	23 November 2026	Remediation Planned	Full or Targeted Retest	Add a timestamp and nonce (or monotonic event ID) to the si...
TMG-WAPT-016	Platform Security Lead	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Add server-side file-signature (magic-byte) validation and...
TMG-WAPT-017	Director, Billing Platform	31-60 Days	23 November 2026	Open	Full or Targeted Retest	Enforce atomic, database-level uniqueness/locking on redemp...
TMG-WAPT-018	Platform Engineering Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Disable or genericize version-disclosing headers at the fra...
TMG-WAPT-019	Identity & Access Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Adopt generic validation messaging consistent with the enum...
TMG-WAPT-020	Platform Engineering Lead	61-90 Days	08 December 2026	Remediation Planned	Full or Targeted Retest	Include Referrer-Policy in the centralized security-header...
TMG-WAPT-021	Front-End Engineering Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Extend the existing build-time log-stripping step to cover...
TMG-WAPT-022	Front-End Engineering Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Update the logout handler to clear the full application sto...
TMG-WAPT-023	Front-End Engineering Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Update the user-facing help text to match the current enfor...
TMG-WAPT-024	Platform Security Lead	61-90 Days	08 December 2026	Open	Full or Targeted Retest	Configure an explicit HTTP method allow-list at the CDN/WAF...
TMG-WAPT-025	Platform Security Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Publish a security.txt file per the informal community conv...
TMG-WAPT-026	API Platform Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Maintain a periodic review process to ensure internal-only...
TMG-WAPT-027	Platform Engineering Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	No dedicated action beyond the header-suppression work alre...
TMG-WAPT-028	Platform Engineering Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Bundle Permissions-Policy into the TMG-WAPT-013 header roll...
TMG-WAPT-029	Front-End Engineering Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Optional: strip build-identifier comments from production b...
TMG-WAPT-030	Platform Security Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Update internal session-management documentation to reflect...
TMG-WAPT-031	Security Operations Lead	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Add a dedicated alert rule for self-targeted role-change at...
TMG-WAPT-032	VP Engineering	Backlog — Defense-in-Depth	Backlog — Next Planning Cycle	Open	Documentation / Config Review	Consider a layered authorization pattern (step-up confirmat...

44 RETEST RECOMMENDATIONS

TMG Security recommends a structured retest following remediation, applying the methodology below. This section describes the recommended retest approach for this fictional engagement; it does not state that remediation has actually occurred.

Recommended Retest Scope

- Full retest of both Critical findings (TMG-WAPT-001, TMG-WAPT-002) and all six High findings (TMG-WAPT-003 through TMG-WAPT-008), including regression testing across related endpoints.
- Targeted retest of each Medium finding against its specific affected endpoint or workflow.
- Confirmation-only review of Low and Informational items, batched into the next general assessment cycle where full retest is not independently warranted.

Retest Methodology

- Evidence Review — confirm that a code or configuration change addressing the finding's root cause has been deployed to the fictional test environment.
- Vulnerability Reproduction — attempt the original safe PoC steps to confirm the previously observed fictional behavior no longer occurs.
- Regression Testing — verify the fix did not introduce a new fictional weakness in adjacent functionality.
- Closure Criteria — a finding is marked Closed only after reproduction confirms remediation and regression testing raises no new concern.

This retest methodology is illustrative. This report does not claim that any finding has been remediated or retested.

45 POSITIVE SECURITY CONTROLS

This fictional assessment is not intended to be entirely negative. TMG Security identified a number of security controls operating effectively across the NorthStar Commerce Portal, summarized below as illustrative fictional observations.

Control Area	Illustrative Observation
Multi-Factor Authentication	MFA is available and functional for privileged roles (Organization Manager, Administrator), with single-use recovery codes and a bounded remembered-device window.
Session Expiration	Access tokens carry a short, appropriate lifetime, and refresh-token rotation invalidates prior tokens on use.
Password Hashing	Fictional password storage uses a modern, appropriately-configured hashing algorithm; no plaintext or reversibly-encrypted password storage was observed.
Security Logging	Authentication and role-change events are captured in centralized fictional logging, supporting the monitoring enhancement noted in TMG-WAPT-031.
Centralized Monitoring	A centralized fictional logging and monitoring platform aggregates security-relevant events across the application tier.
Web Application Firewall	A cloud-based fictional WAF sits in front of the application, providing a baseline layer of edge protection.
Rate Limiting (Partial)	Rate limiting is effectively implemented on the login endpoint, demonstrating the pattern needed elsewhere (see TMG-WAPT-009).
TLS Configuration	TLS configuration disallows deprecated protocol versions and weak cipher suites across tested fictional endpoints.
Security Headers (Partial)	HSTS and X-Content-Type-Options were consistently present, even where other headers require completion (see TMG-WAPT-013).
Access Review Process	A fictional periodic access-review process for Administrator-level accounts was described and evidenced during interviews with the platform team.

All observations above are fictional and were constructed for this illustrative sample assessment.

46 TESTING LIMITATIONS

The following limitations apply to this fictional sample assessment and should be read together with the Important Disclaimer (Section 02).

- NorthStar Digital Commerce, Inc. and NorthStar Commerce Portal are fictional; no real organization or application was assessed.
- No real credentials, cloud credentials, or production systems were used or accessed.
- No real customer data was accessed at any point.
- No production environment was tested; only a fictional staging/controlled assessment environment is represented.
- No destructive testing was performed or simulated as executed.
- No denial-of-service testing was performed.
- No social engineering was performed.
- No physical security testing was performed.
- No real cloud-provider environment or infrastructure was tested.
- No third-party systems were tested.
- All evidence, screenshots, and request/response examples in this report are synthetic.

This report describes a fictional, illustrative testing exercise only.

47 APPENDIX A — TEST CASE REGISTER

The register below documents all 87 fictional test cases executed during this illustrative assessment, spanning 20 testing categories, with a result and cross-reference to any corresponding finding.

Test ID	Category	Objective	Result	Finding
TC-001	Authentication	Verify login rejects invalid credentials with a generic error message.	No Exception Identified	—
TC-002	Authentication	Verify account-lockout / throttling behavior after repeated failed login attempts.	No Exception Identified	—
TC-003	Authentication	Verify login response does not distinguish between invalid username and invalid password.	No Exception Identified	—
TC-004	Authentication	Verify password field is never reflected or logged in cleartext across the login flow.	No Exception Identified	—
TC-005	Authentication	Verify concurrent login attempts from multiple fictional test devices are handled per policy.	No Exception Identified	—
TC-006	Authorization	Verify Standard User cannot access another fictional tenant's organization profile.	Exception Identified	TMG-WAPT-001
TC-007	Authorization	Verify Standard User cannot self-elevate to Organization Manager role.	Exception Identified	TMG-WAPT-006
TC-008	Authorization	Verify Billing User cannot change subscription plan without payment-authorization event.	Exception Identified	TMG-WAPT-002
TC-009	Authorization	Verify Support Agent cannot access billing/subscription management functions.	No Exception Identified	—
TC-010	Authorization	Verify Administrator-only endpoints reject non-administrator sessions.	No Exception Identified	—
TC-011	Authorization	Verify server-side authorization is enforced independent of front-end role-based UI hiding.	Exception Identified	TMG-WAPT-007
TC-012	Session	Verify session cookie carries Secure, HttpOnly, and SameSite attributes.	No Exception Identified	—
TC-013	Session	Verify access token is rejected immediately following an explicit logout.	Exception Identified	TMG-WAPT-010
TC-014	Session	Verify refresh-token rotation invalidates the prior refresh token on use.	No Exception Identified	—
TC-015	Session	Verify concurrent-session behavior across two fictional test devices matches documented policy.	No Exception Identified	—
TC-016	Session	Verify local-storage state is fully cleared following logout.	Exception Identified	TMG-WAPT-022
TC-017	Access Control	Verify direct object references (file IDs) cannot be used to access another tenant's fictional file.	Exception Identified	TMG-WAPT-008
TC-018	Access Control	Verify organization-scoped API endpoints derive tenant context from session, not request parameters.	Exception Identified	TMG-WAPT-001
TC-019	Access Control	Verify member-directory API applies role-aware field scoping.	Exception Identified	TMG-WAPT-007
TC-020	Access Control	Verify administrative dashboard routes are unreachable without an Administrator session.	No Exception Identified	—
TC-021	Input Validation	Verify malformed JSON input returns a generic, non-verbose error response.	Exception Identified	TMG-WAPT-012
TC-022	Input Validation	Verify oversized request payloads are rejected with an appropriate error code.	No Exception Identified	—
TC-023	Input Validation	Verify unexpected/unused fields in request bodies are ignored rather than bound to internal models.	Exception Identified	TMG-WAPT-014
TC-024	Input Validation	Verify parameter-pollution (duplicate query parameters) does not alter authorization outcome.	No Exception Identified	—
TC-025	Injection	Verify SQL-injection-style fictional payloads in search/filter parameters are safely parameterized.	No Exception Identified	—
TC-026	Injection	Verify NoSQL-injection-style fictional payloads in filter objects do not alter query logic.	No Exception Identified	—
TC-027	Injection	Verify OS command-injection-style fictional payloads in file-name fields are rejected/sanitized.	No Exception Identified	—
TC-028	Injection	Verify server-side template-injection-style fictional payloads in user-supplied text fields are not evaluated.	No Exception Identified	—
TC-029	Injection	Verify stored HTML/script content in support-ticket comments is encoded on output in all rendering contexts.	Exception Identified	TMG-WAPT-003
TC-030	Injection	Verify path-traversal-style fictional payloads in file-reference parameters are rejected.	No Exception Identified	—
TC-031	Business Logic	Verify subscription plan-tier transitions require an authoritative server-side payment event.	Exception Identified	TMG-WAPT-002
TC-032	Business Logic	Verify single-use discount codes cannot be redeemed twice via rapid-sequence requests.	Exception Identified	TMG-WAPT-017
TC-033	Business Logic	Verify invoice state transitions follow the defined workflow order (draft → issued → paid).	No Exception Identified	—
TC-034	Business Logic	Verify email-verification workflow cannot be bypassed via direct API state manipulation.	No Exception Identified	—
TC-035	Business Logic	Verify organization-ownership transfer requires confirmation from the receiving fictional account.	No Exception Identified	—
TC-036	Business Logic	Verify notification-triggering events match actual enforcement state (no notify/enforce mismatch).	No Exception Identified	—
TC-037	API	Verify object-level authorization (BOLA) on all organization- and file-scoped API endpoints.	Exception Identified	TMG-WAPT-001, TMG-WAPT-008
TC-038	API	Verify function-level authorization on privileged API actions (role change, plan change).	Exception Identified	TMG-WAPT-006
TC-039	API	Verify API responses do not include excessive fields beyond the requesting role's authorization.	Exception Identified	TMG-WAPT-007

Test ID	Category	Objective	Result	Finding
TC-040	API	Verify API endpoints correctly enforce rate limiting on high-value/expensive operations.	Exception Identified	TMG-WAPT-009
TC-041	API	Verify API error responses use a consistent, non-verbose error envelope.	Exception Identified	TMG-WAPT-012
TC-042	File Upload	Verify file-type validation relies on server-side content inspection, not client-supplied metadata.	Exception Identified	TMG-WAPT-016
TC-043	File Upload	Verify uploaded files are stored outside the web root with authorization-gated retrieval.	No Exception Identified	—
TC-044	File Upload	Verify uploaded filenames are sanitized to prevent path traversal on storage.	No Exception Identified	—
TC-045	File Upload	Verify file-download signed URLs enforce organization-ownership checks.	Exception Identified	TMG-WAPT-008
TC-046	Password Reset	Verify password-reset tokens expire within the documented window.	No Exception Identified	—
TC-047	Password Reset	Verify password-reset tokens cannot be reused after successful completion.	No Exception Identified	—
TC-048	Password Reset	Verify password-reset-request endpoint enforces application-level rate limiting.	Exception Identified	TMG-WAPT-009
TC-049	Password Reset	Verify email-change confirmation codes are bound to their originating change-request.	Exception Identified	TMG-WAPT-004
TC-050	MFA	Verify MFA is enforced at login for accounts with MFA enabled, with no bypass path.	No Exception Identified	—
TC-051	MFA	Verify MFA enrollment is available and functional for Administrator and Organization Manager roles.	No Exception Identified	—
TC-052	MFA	Verify MFA recovery-code usage is single-use and logged.	No Exception Identified	—
TC-053	MFA	Verify "remembered device" duration for MFA is bounded and independently configurable.	No Exception Identified	—
TC-054	CORS	Verify CORS Access-Control-Allow-Origin reflects only the explicit, active front-end origin set.	Exception Identified	TMG-WAPT-011
TC-055	CORS	Verify Access-Control-Allow-Credentials is not combined with a wildcard or overly broad origin pattern.	Exception Identified	TMG-WAPT-011
TC-056	CORS	Verify preflight (OPTIONS) responses do not leak sensitive routing detail.	No Exception Identified	—
TC-057	Headers	Verify Content-Security-Policy is present and appropriately scoped.	Exception Identified	TMG-WAPT-013
TC-058	Headers	Verify X-Content-Type-Options: nosniff is present on all responses.	No Exception Identified	—
TC-059	Headers	Verify HSTS is present with an appropriate max-age on all HTTPS responses.	No Exception Identified	—
TC-060	Headers	Verify Referrer-Policy is explicitly set platform-wide.	Exception Identified	TMG-WAPT-020
TC-061	Headers	Verify Permissions-Policy is set to restrict unused browser features.	Exception Identified	TMG-WAPT-028
TC-062	SSRF	Verify webhook-validation feature restricts outbound destinations via an egress allow-list.	Exception Identified	TMG-WAPT-005
TC-063	SSRF	Verify remote-image-import feature (where present) blocks private/link-local address ranges.	No Exception Identified	—
TC-064	SSRF	Verify URL-preview feature does not follow redirects into private IP ranges.	No Exception Identified	—
TC-065	Webhooks	Verify outbound webhook payloads are signed with a verifiable signature.	No Exception Identified	—
TC-066	Webhooks	Verify webhook signature scheme incorporates timestamp/nonce to prevent replay.	Exception Identified	TMG-WAPT-015
TC-067	Webhooks	Verify webhook event delivery includes a stable, de-duplicable event identifier.	No Exception Identified	—
TC-068	Webhooks	Verify webhook configuration is restricted to Organization Manager and Administrator roles.	No Exception Identified	—
TC-069	Rate Limiting	Verify login endpoint enforces rate limiting with exponential backoff.	No Exception Identified	—
TC-070	Rate Limiting	Verify password-reset-request endpoint enforces rate limiting.	Exception Identified	TMG-WAPT-009
TC-071	Rate Limiting	Verify registration/invitation endpoints enforce reasonable request-volume limits.	No Exception Identified	—
TC-072	Rate Limiting	Verify expensive API operations (report generation, bulk export) enforce request throttling.	No Exception Identified	—
TC-073	Client-Side	Verify sensitive tokens are not stored in browser localStorage in cleartext.	No Exception Identified	—
TC-074	Client-Side	Verify production front-end bundle does not retain verbose debug logging.	Exception Identified	TMG-WAPT-021
TC-075	Client-Side	Verify front-end source maps are not published for the production bundle.	No Exception Identified	—
TC-076	Client-Side	Verify client-side role checks are mirrored by equivalent server-side enforcement.	Exception Identified	TMG-WAPT-007
TC-077	Server-Side	Verify server-side authorization is independently enforced on every privileged action.	Exception Identified	TMG-WAPT-006
TC-078	Server-Side	Verify framework default/debug endpoints are disabled in the production configuration.	No Exception Identified	—
TC-079	Server-Side	Verify unused HTTP methods are explicitly disabled at the edge layer.	Exception Identified	TMG-WAPT-024
TC-080	Server-Side	Verify server-side request timeout and resource limits are configured for public endpoints.	No Exception Identified	—
TC-081	Error Handling	Verify unhandled exceptions return a generic client-facing error envelope.	Exception Identified	TMG-WAPT-012
TC-082	Error Handling	Verify stack traces and internal file paths are never returned to the client.	Exception Identified	TMG-WAPT-012
TC-083	Error Handling	Verify registration validation messaging does not distinguish account-existence signals.	Exception Identified	TMG-WAPT-019
TC-084	Configuration	Verify version-disclosing response headers are suppressed in production.	Exception Identified	TMG-WAPT-018
TC-085	Configuration	Verify directory listing is disabled across all static-asset paths.	No Exception Identified	—
TC-086	Configuration	Verify a security.txt vulnerability-disclosure file is published.	Exception Identified	TMG-WAPT-025
TC-087	Configuration	Verify TLS configuration disallows deprecated protocol versions and weak cipher suites.	No Exception Identified	—

48 APPENDIX B — ENDPOINT REGISTER

The register below documents all 34 fictional endpoints identified during attack-surface mapping (Section 10), with method, authentication, role, function, and testing result.

Endpoint	Method	Auth	Role	Function	Tested	Result	Finding Ref.
/login	POST	None	Unauthenticated Visitor	Session issuance (email/password)	Yes	Reviewed	WAPT-009 (related pattern)
/register	POST	None	Unauthenticated Visitor	Account creation	Yes	Finding	WAPT-019
/logout	POST	Session	Standard User	Session termination	Yes	Finding	WAPT-010, WAPT-022
/password-reset	POST	None	Unauthenticated Visitor	Password-reset request	Yes	Finding	WAPT-009
/api/v1/account/password-reset/request	POST	None	Unauthenticated Visitor	Password-reset request (API)	Yes	Finding	WAPT-009
/api/v1/account/email-change	POST	Session	Standard User	Email-change confirmation	Yes	Finding	WAPT-004
/profile	GET/PATCH	Session	Standard User	User profile view/update	Yes	Clean	—
/api/v1/users/{id}	GET	Session	Standard User	User object retrieval	Yes	Clean	—
/organizations	GET	Session	Standard User	Organization listing	Yes	Clean	—
/organizations/{id}	GET	Session	Standard User	Organization detail	Yes	Finding	WAPT-001
/api/v1/organizations/{orgId}/profile	GET/PATCH	Session	Org Manager	Organization profile	Yes	Finding	WAPT-001, WAPT-014
/members	GET	Session	Standard User	Member directory (UI)	Yes	Clean	—
/api/v1/organizations/{orgId}/members	GET	Session	Standard User	Member directory (API)	Yes	Finding	WAPT-007
/api/v1/organizations/{orgId}/members/{userId}/role	PATCH	Session	Org Manager	Member role assignment	Yes	Finding	WAPT-006
/billing	GET	Session	Billing User	Billing dashboard	Yes	Clean	—
/api/v1/billing/subscriptions/{subId}/plan	POST	Session	Billing User	Subscription plan change	Yes	Finding	WAPT-002
/invoices	GET	Session	Billing User	Invoice listing	Yes	Clean	—
/api/v1/billing/invoices/{id}	GET	Session	Billing User	Invoice detail	Yes	Clean	—
/subscriptions	GET	Session	Billing User	Subscription overview	Yes	Clean	—
/api/v1/billing/discounts/redeem	POST	Session	Billing User	Discount-code redemption	Yes	Finding	WAPT-017
/files	GET	Session	Standard User	File listing	Yes	Clean	—
/api/v1/files/upload	POST	Session	Standard User	File upload	Yes	Finding	WAPT-016
/api/v1/files/{fileId}/download	GET	Session	Standard User	File download (signed URL)	Yes	Finding	WAPT-008
/support	GET	Session	Standard User	Support ticket list	Yes	Clean	—
/api/v1/support/tickets/{id}/comments	POST	Session	Standard User	Ticket comment submission	Yes	Finding	WAPT-003
/notifications	GET	Session	Standard User	Notification center	Yes	Clean	—
/api/v1/webhooks	GET/POST	Session	Org Manager	Webhook subscription management	Yes	Finding	WAPT-015
/api/v1/webhooks/validate	POST	Session	Org Manager	Webhook destination validation	Yes	Finding	WAPT-005
/admin	GET	Session	Administrator	Administrative dashboard	Yes	Clean	—
/api/v1/users	GET	Session	Administrator	Platform-wide user listing	Yes	Clean	—
/api/v1/organizations	GET	Session	Administrator	Platform-wide organization listing	Yes	Clean	—
/api/v1/billing	GET	Session	Administrator/Billing User	Platform billing overview	Yes	Clean	—
/api/v1/docs	GET	None	Unauthenticated Visitor	Interactive API documentation	Yes	Finding	WAPT-026
/.well-known/security.txt	GET	None	Unauthenticated Visitor	Vulnerability disclosure metadata	Yes	Finding	WAPT-025

49 APPENDIX C — FINDING REGISTER

The complete register of all 32 fictional findings is provided below for traceability against Sections 34-38 and the Management Action Plan (Section 43).

Finding ID	Title	Severity	CVSS	Status	Ref.
TMG-WAPT-001	Broken Object-Level Authorization Leading to Cross-Tenant Customer Data Access	CRITICAL	9.1	Remediation In Progress	§34
TMG-WAPT-002	Business Logic Authorization Bypass Allowing Unauthorized Subscription Privilege Escalation	CRITICAL	9.0	Remediation In Progress	§34
TMG-WAPT-003	Stored Cross-Site Scripting in Customer Support Workflow	HIGH	8.2	Open	§35
TMG-WAPT-004	Account Recovery Workflow Allows Unauthorized Email Change	HIGH	7.9	Open	§35
TMG-WAPT-005	Server-Side Request Forgery in Webhook Validation Feature	HIGH	8.1	Remediation Planned	§35
TMG-WAPT-006	Privilege Escalation from Standard User to Organization Manager	HIGH	7.6	Remediation In Progress	§35
TMG-WAPT-007	Excessive API Data Exposure Through Organization Endpoint	HIGH	7.3	Open	§35
TMG-WAPT-008	File Download Authorization Bypass	HIGH	7.1	Open	§35
TMG-WAPT-009	Insufficient Rate Limiting on Password Reset Endpoint	MEDIUM	5.9	Remediation Planned	§36
TMG-WAPT-010	JWT / Session Revocation Weakness	MEDIUM	6.3	Open	§36
TMG-WAPT-011	CORS Trusts Unnecessary Origins	MEDIUM	5.4	Remediation Planned	§36
TMG-WAPT-012	Verbose Error Messages Reveal Internal Application Details	MEDIUM	5.3	Open	§36
TMG-WAPT-013	Missing Security Header Defense	MEDIUM	5.0	Remediation Planned	§36
TMG-WAPT-014	Mass Assignment in Organization Profile Update	MEDIUM	6.1	Open	§36
TMG-WAPT-015	Webhook Replay Protection Missing	MEDIUM	5.7	Remediation Planned	§36
TMG-WAPT-016	Insufficient File Validation	MEDIUM	5.6	Open	§36
TMG-WAPT-017	Business Logic Replay in Discount Workflow	MEDIUM	5.8	Open	§36
TMG-WAPT-018	Technology Version Disclosure	LOW	3.1	Open	§37
TMG-WAPT-019	Verbose Validation Response	LOW	2.9	Open	§37
TMG-WAPT-020	Missing Referrer-Policy Hardening	LOW	2.6	Remediation Planned	§37
TMG-WAPT-021	Unnecessary Client-Side Debug Logging	LOW	2.8	Open	§37
TMG-WAPT-022	Logout Does Not Immediately Clear One Non-Privileged Local Session Artifact	LOW	2.5	Open	§37
TMG-WAPT-023	Password Policy Documentation Inconsistency	LOW	2.2	Open	§37
TMG-WAPT-024	Security Configuration Hardening Opportunity	LOW	3.0	Open	§37
TMG-WAPT-025	Security.txt Not Present	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-026	API Documentation Exposure — Intended but Reviewable	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-027	Detailed Technology Fingerprinting	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-028	Unused Security Response Header Opportunity	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-029	Exposed Non-Sensitive Build Metadata	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-030	Session Management Documentation Improvement	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-031	Security Monitoring Enhancement Opportunity	INFORMATIONAL	N/A	Open	§38
TMG-WAPT-032	Defense-in-Depth Recommendation for Sensitive Workflows	INFORMATIONAL	N/A	Open	§38

50 APPENDIX D — TEST ACCOUNT REGISTER

The fictional test accounts below were used throughout this assessment. No real passwords are recorded in this report; all credential values are placeholders.

Fictional Account	Role	User ID	Organization	Credential
wapt.user01@example.test	Standard User	TEST-USER-1001	ORG-1001	*[Fictional Test Credential]*
wapt.billing01@example.test	Billing User	USER-2200	ORG-1001	*[Fictional Test Credential]*
wapt.manager01@example.test	Organization Manager	USER-3100	ORG-1001	*[Fictional Test Credential]*
wapt.support01@example.test	Support Agent	USER-4400	ORG-1001	*[Fictional Test Credential]*
wapt.admin01@example.test	Administrator	USER-9900	Platform-Wide	*[Fictional Test Credential]*
wapt.user02@example.test	Standard User	USER-5502	ORG-1002	*[Fictional Test Credential]*

Illustrative Purpose column (per account):

- wapt.user01@example.test — Primary standard-user test account, ORG-1001.
- wapt.billing01@example.test — Billing workflow and subscription testing.
- wapt.manager01@example.test — Role management and organization-profile testing.
- wapt.support01@example.test — Support-ticket workflow testing.
- wapt.admin01@example.test — Administrative dashboard and platform-wide function testing.
- wapt.user02@example.test — Secondary tenant account used for cross-tenant isolation testing.

All accounts, identifiers, and credential placeholders above are fictional. No real credentials are recorded anywhere in this report.

51 APPENDIX E — METHODOLOGY NOTES

This appendix provides supplementary detail on how each stage of TMG Security's methodology (Section 08) was applied during this fictional assessment.

Reconnaissance

Passive review of publicly reachable pages and metadata, combined with light active enumeration of the fictional staging environment, consistent with the non-destructive rules of engagement.

Enumeration

Systematic walkthrough of the fictional application's functionality and API surface across all six defined roles, producing the endpoint register in Appendix B.

Authenticated Testing

The majority of testing was performed authenticated, using the dedicated fictional test accounts in Appendix D, reflecting the reality that most real-world web application risk lives behind authentication.

Role-Based Testing

Each testing category was repeated across relevant roles to independently validate horizontal and vertical authorization boundaries, rather than relying on a single privileged account throughout.

API Testing

API endpoints were tested both through the front-end application and via direct API calls, to ensure server-side enforcement was validated independent of client-side behavior.

Business Logic Analysis

Multi-step fictional workflows were mapped and tested for state-manipulation and sequence-bypass conditions that conventional input-validation testing does not reliably surface.

Manual Testing & Validation

Every candidate finding was manually validated by a TMG Security fictional tester before inclusion in this report; no automated-scanner output was included without manual confirmation.

Evidence Collection

All fictional evidence was captured and referenced using the EV-WAPT-### identifiers cited throughout Sections 34-38, maintaining traceability from finding to evidence.

Reporting

Findings were documented using the consistent format defined in Section 33, then reconciled across the Dashboard, Findings Summary, Detailed Findings, Finding Register, and Management Action Plan to ensure full internal consistency.

52 FINAL CONCLUSION

Illustrative Security Assessment Conclusion

> *"NorthStar Commerce Portal demonstrates a number of established security controls, but the fictional assessment identified material weaknesses in authorization, business logic enforcement, account recovery, API access control, and selected defensive controls."*

The two Critical and six High fictional findings in this sample report require immediate attention and should be the organization's first priority, given their concentration around authorization and trust-boundary enforcement. The nine Medium findings should be integrated into the standard remediation backlog and addressed within the illustrative 31-60 day window. The seven Low and eight Informational findings support defense-in-depth improvements and do not represent an immediate exploitation path in this fictional sample, but should not be indefinitely deferred.

TMG Security's simulated recommendation is that NorthStar retest all Critical and High findings following remediation, per the methodology in Section 44, before considering this fictional assessment's core concerns resolved. A follow-on

assessment cycle — informed by the maturity and monitoring recommendations in Sections 45 and Appendix E — is recommended within twelve months.

THIS IS A FICTIONAL SAMPLE ASSESSMENT.

53 CONTACT & DISCLAIMER

Cybersecurity | *SOC* | *VAPT* | *GRC* | *MDR* | *Compliance Solutions* | *Corporate Trainings*
Web: www.tmgsec.com **Email:** security@tmgsec.com
USA Office: 117 South Lexington Street, STE 100, Harrisonville, MO 64701
Support: support@tmgsec.com | **Phone:** +1 (816) 793-1929
WhatsApp: +1 (480) 680-0342

Final Disclaimer

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL CLIENT PENETRATION TEST

This report was created by TMG Security solely to demonstrate web application penetration-testing methodology, technical reporting standards, evidence presentation, and remediation guidance. NorthStar Digital Commerce, Inc. and NorthStar Commerce Portal are fictional. No real client environment was assessed. No real credentials, personal data, production systems, or customer information were accessed. All vulnerabilities, requests, responses, screenshots, findings, severity ratings, and remediation actions are illustrative.