MUT3D

CYBERSECURITY

REPORT / v3.0

PENETRATION TEST REPORT

Web application / External assessment

CLIENT	ACME.COM / fictional case study
REPORT ID	MUT3D-ACME-2026-001
WINDOW	20-24 Oct 2026 / illustrative
STATUS	Sample document / no live testing

ILLUSTRATIVE SAMPLE / NO CLIENT DATA

Report contents

01	Executive summary	03
02	Scope and coverage	04
03	Findings register	06
04	Detailed findings	07
05	Remediation and retest	12
06	Evidence and rating model	14

ACME.COM is an illustrative client name. Assets use reserved example domains.

DOCUMENT CONTROL

Report at a glance

A realistic report structure with invented data for evaluating our deliverables.

Report identifier	**MUT3D-ACME-2026-001**
Assessment type	**Web application and API security review**
Illustrative client	**ACME.COM**
Testing window	**20-24 October 2026**
Report issue	**03 November 2026 / version 3.0**
Classification	**Public sample - fictional content**

READER GUIDE

How to use this report

Leadership can use the risk summary and roadmap to prioritize work. Engineering teams can use the finding IDs, affected components, evidence descriptions, and verification criteria to plan remediation. The assessment scope and limitations determine what conclusions can be drawn.

All entities, findings, dates, counts, and observations in this document are fictional. No testing of acme.com or related systems was performed.

01 / EXECUTIVE SUMMARY

A focused risk picture

Four fictional findings across two reserved example assets.

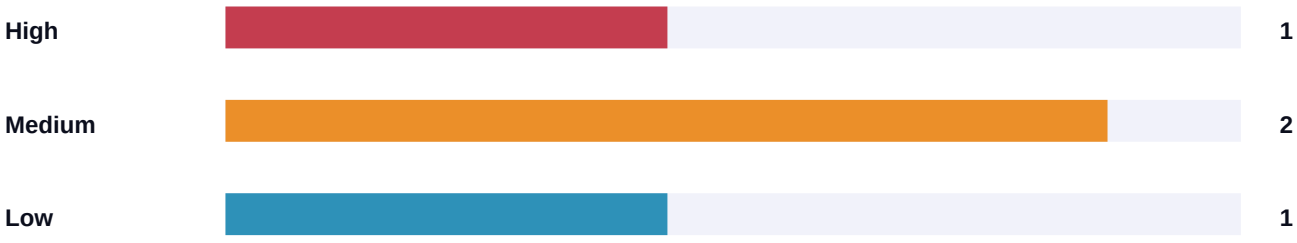
OVERALL ASSESSMENT

One access-control weakness warrants priority remediation. Two workflow controls need strengthening. One hardening gap can follow in the normal release cycle.

01	02	01	04
HIGH	MEDIUM	LOW	TOTAL

RISK DISTRIBUTION

Validated findings by severity



Management priority: F-01 should enter an expedited release because it crosses a customer data boundary. F-02 and F-03 can follow in the next planned release after their owners agree the session and request policies. F-04 belongs in routine configuration hardening. This order is an illustrative decision, not a service-level commitment.

02 / SCOPE

Defined assets and boundaries

Conclusions in a real engagement apply only to assets explicitly authorized for testing.

AUTHORIZED TARGETS

Illustrative scope register

portal.acme.example Authentication, accounts, documents	Customer portal
api.acme.example Session, object access, request controls	Application API

TEST IDENTITIES

Synthetic roles

The scenario models two separate customer tenants, a support role with scoped access, and a read-only analyst role. Each account has synthetic documents and event history. Role comparisons cover direct navigation, document preview, session renewal, and API access. Written authorization and a test window are assumed for this fictional engagement.

EXCLUSIONS

Outside this assessment

Production infrastructure, third-party providers, employee accounts, social engineering, denial-of-service testing, source code, and any asset outside the two reserved example domains. The sample does not establish the security of untested routes or integrations.

02 / COVERAGE

What the team examined

The chart illustrates a staged assessment rather than instantaneous scanning.

COVERAGE MATRIX

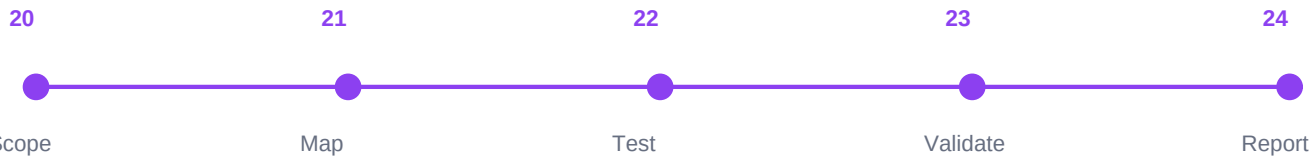
Workstreams and outcome

Authentication	Reviewed	**F-02**
Object authorization	Finding	**F-01**
API request controls	Finding	**F-03**
Response hardening	Finding	**F-04**
Business workflows	Reviewed	**-**

The matrix records where review produced a finding and where a workstream was examined without a reported issue. "Reviewed" does not mean every possible weakness was excluded.

ACTIVITY / 20-24 OCT

Illustrative assessment timeline



Activity is staged: scoping, surface mapping, testing, manual validation, and reporting. Findings are reviewed before delivery.

03 / FINDINGS REGISTER

Priorities at a glance

Identifiers remain stable through remediation and any agreed retest.

ID	SEVERITY	FINDING	ASSET
F-01	HIGH	Cross-account document access	Portal
F-02	MEDIUM	Session persists after reset	Portal
F-03	MEDIUM	Uneven request controls	API
F-04	LOW	Response hardening gap	Portal

RISK PRIORITY

Impact versus effort

F-01	High impact / Medium effort
F-02	Medium impact / Low effort
F-03	Medium impact / Medium effort
F-04	Low impact / Low effort

The rating reflects the fictional scenario and is not a CVSS score. See the rating model on page 15.

04 / DETAILED FINDING / F-01

Cross-account document access

A missing ownership check affects an account document workflow.

F-01 / HIGH

portal.acme.example / Authorization

OBSERVATION

The synthetic portal listed only documents assigned to account A. A separate document retrieval path nevertheless returned a document assigned to account B while the reviewer was using account A. The result was checked against the tenant ownership matrix and repeated in the invented test record. This is an application authorization boundary, not a presentation defect.

IMPACT

The fictional document contains customer account material. In a real service, crossing this boundary could expose another tenant's records and create a privacy or contractual incident. The actual impact would depend on document sensitivity, identifier availability, logging, and whether other document functions share the same control. The sample does not assert those conditions for a live service.

EVIDENCE / SYNTHETIC / EV-01

SESSION	DOCUMENT OWNER	OBSERVED RESULT
Account A	Account A	**Allowed / expected**
Account A	Account B	**Allowed / unexpected**

RECOMMENDED CHANGE

Enforce one server-side ownership or sharing policy for list, detail, preview, and export. Check the authenticated principal before retrieving content, and cover each role in regression tests.

RETEST CRITERION

Account A must be denied access to account B material. The owner and any explicitly shared role must retain their intended access. Record the build and evidence ID.

04 / F-01 / CORRECTIVE ACTION

Close the ownership gap

The remediation record connects the finding to an observable verification result.

ROOT CAUSE / HYPOTHESIS

UI filtering without matching server control

The fictional portal applies account filtering to its document list, while the retrieval flow trusts the selected document identifier. The engineering team should confirm this boundary in code review.

RECOMMENDED CHANGE

Centralize access checks

Use one server-side policy for document listing, detail, preview, and export. Reject access before content retrieval. Avoid relying on client-visible identifiers as authorization.

RETEST CRITERIA

Owner allowed; other account denied

Run the same synthetic account pair after the change. Record the decision, status, and evidence reference. Check role-specific sharing rules and regression tests.

Suggested owner: application engineering. Suggested priority: next emergency or expedited release, subject to real-world impact assessment.

04 / DETAILED FINDING / F-02

Session persists after reset

Existing sessions remain active after a credential change in the fictional flow.

F-02 / MEDIUM

portal.acme.example / Session lifecycle

OBSERVATION

In the fictional recovery flow, account A completed a password reset at 09:12. A session issued before that reset was still accepted at 09:13 and continued to reach account pages. The reviewer compared the pre-reset and post-reset states using the same synthetic identity. The case tests the expected session lifecycle; it does not claim that a session was stolen.

IMPACT

A credential reset is often used when a user suspects exposure. If earlier sessions remain valid without a clear revocation policy, the reset may not end access already established on another device. Exposure depends on session duration, device visibility, additional authentication, and the ability to revoke all sessions. These conditions would be checked before a real severity decision.

EVIDENCE / SYNTHETIC / EV-02

EV-02 links the reset completion event, the earlier session identifier in redacted form, the observed acceptance after reset, and the reviewer's timestamped note. The exhibit on page 16 shows the sequence without credentials or token values.

RECOMMENDED CHANGE

Define and implement a reset-time session policy. Revoke prior sessions or provide a visible account-wide revocation action, and document any deliberate exceptions.

RETEST CRITERION

The earlier session must be rejected after reset. A newly established session should work normally, and the event should appear in account security logs.

04 / DETAILED FINDING / F-03

Uneven request controls

Sensitive API actions lack consistent throttling in the fictional scenario.

F-03 / MEDIUM

api.acme.example / Request controls

OBSERVATION

The synthetic API applies a control point to account recovery requests, while invite issuance continues accepting a larger share of requests in the same illustrative window. The reviewer compared policy outcomes and response categories, not system throughput. The difference suggests that the two sensitive workflows use separate configurations or incomplete shared middleware.

IMPACT

An uneven policy can create avoidable notification volume, support load, or abuse opportunities. It may also make monitoring less reliable when one workflow generates alerts and the other does not. Actual impact depends on account discovery protections, recipient limits, challenge mechanisms, and downstream notification behavior. No real service or person received messages in this sample.

EVIDENCE / SYNTHETIC / EV-03

EV-03 stores aggregate counts, response categories, a sanitized control state, and the approved synthetic test window. Page 16 visualizes the relative difference. The exhibit intentionally omits target identities and request contents.

RECOMMENDED CHANGE

Agree a shared policy for sensitive actions, apply it consistently, and add telemetry that distinguishes normal retries from unusual repetition without exposing user details.

RETEST CRITERION

Both workflows must reach the agreed control state under the same test conditions. Alerts and logs must identify the controlled action accurately.

04 / DETAILED FINDING / F-04

Response hardening gap

A subset of portal responses omits a planned security header.

F-04 / LOW

portal.acme.example / Configuration

OBSERVATION

The fictional portal returns its planned browser response policy on the main application pages. A document preview route follows a separate configuration and omits one of those headers. The reviewer compared the route classes on the same illustrative build and found no basis for treating static assets as the same issue. The difference is limited to the preview path in this sample.

IMPACT

The missing header reduces consistency of browser-side hardening on a route that handles customer documents. It is a defense-in-depth gap, and the sample does not show a standalone compromise or direct data exposure from this omission. A real rating would consider the content type, rendering behavior, and any compensating controls before prioritizing the change.

EVIDENCE / SYNTHETIC / EV-04

EV-04 contains a sanitized comparison of response policy by route class and a note about the configuration boundary. Page 17 shows the difference. No document body or customer identifier is included.

RECOMMENDED CHANGE

Bring preview responses under the agreed header policy and validate the change against supported document rendering, caching, and download behavior.

RETEST CRITERION

Representative preview responses must include the policy, while document rendering still works. Record the configuration version and regression result.

05 / REMEDIATION

A practical action plan

Order the work by impact, dependency, and confidence in the fix.

Priority 1 — **0-7 days**

F-01 / ownership enforcement

Priority 2 — **Next release**

F-02 session revocation; F-03 request controls

Routine — **Planned hardening**

F-04 response policy alignment

F-01 is a prerequisite for declaring customer document isolation effective. F-02 and F-03 can proceed in parallel after the session and request policies are agreed. F-04 has no dependency on the other fixes.

OWNER MATRIX

Who does what

Application engineering	F-01 and F-02 corrective changes
Platform engineering	F-03 API controls and telemetry
Web operations	F-04 response configuration
Security reviewer	Retest evidence and closure decision

05 / VERIFICATION

Retest and closure

A finding is closed when the agreed behavior is demonstrated, not when a ticket is marked done.

F-01	Cross-account document access denied; owner access retained.
F-02	Earlier sessions rejected after password reset.
F-03	Sensitive API flows follow the agreed request policy.
F-04	Response policy present on representative portal routes.

For each retest, the reviewer records the build identifier, test identity, expected behavior, observed behavior, evidence reference, and a closure decision. Any residual risk is written back to the finding record.

LIMITATIONS

What this document does not prove

This is a fictional demonstration of report structure, not an assessment of acme.com. It provides no assurance about any real system. A real report would contain signed scope, actual test dates, validated evidence, tailored impact, and client-approved distribution controls.

06 / EVIDENCE REGISTER

Traceability without exposure

Each finding points to a controlled evidence set; this public sample contains only synthetic summaries.

REF	FINDING	MATERIAL	HANDLING
EV-01	F-01	Two-account access comparison	Redacted
EV-02	F-02	Session state before and after reset	No tokens
EV-03	F-03	Aggregate request-control observations	No secrets
EV-04	F-04	Response policy comparison	Headers only

CHAIN OF REVIEW

How evidence supports a conclusion

A reviewer compares the observed result with the authorized role matrix, checks that the observation is repeatable inside the agreed test window, and records uncertainty before assigning severity. Raw material belongs in a restricted evidence store. The client-facing report carries only the minimum details needed to explain and reproduce a confirmed issue.

No live traffic, real credentials, or real customer documents were used to create this sample.

06 / RATING MODEL

How priority is assigned

Severity combines plausible impact with the conditions required for the issue to matter.

IMPACT

High

Cross-tenant data boundary

LIKELIHOOD

Conditional

Requires an authenticated user

CONFIDENCE

Illustrative

No real validation was performed

PRIORITY

Expedited

F-01 takes the first fix window

ASSESSMENT RULES

Interpretation and limits

The four ratings are editorial illustrations. A production assessment would consider exploit preconditions, affected data, authorization boundaries, compensating controls, business criticality, and the quality of the evidence. A numerical score would be calculated only when the relevant inputs are known. Remediation windows are discussed with the client and may change as the investigation progresses.

SAMPLE INTEGRITY

ACME.COM is a fictional client in this document. The reserved .example assets are not real targets.

06 / EVIDENCE EXHIBITS

Session and control traces

These exhibits show the type of comparison a real report would preserve as evidence.

EV-02 / SESSION LIFECYCLE

State after a credential reset



Expected behavior: the pre-reset session is revoked under the illustrated policy. Observed behavior: the synthetic session remained valid. The report would retain the timestamped state comparison and omit token values.

EV-03 / REQUEST CONTROLS

Consistency across two workflows



SYNTHETIC SHARE OF REQUESTS ACCEPTED AFTER THE CONTROL POINT

The chart compares policy behavior, not system capacity. The different outcomes prompted F-03. A real report would document the approved volume, response pattern, monitoring signals, and any compensating safeguards.

06 / EVIDENCE EXHIBITS

Configuration comparison

A concise appendix ties the hardening observation to a concrete route difference.

EV-04 / RESPONSE POLICY

Representative route comparison

ROUTE CLASS	POLICY	RESULT
Main portal pages	Expected header present	**Consistent**
Document preview	Expected header absent	**Review**
Static assets	Covered separately	**No finding**

INTERPRETATION

Evidence, inference, and limits

The observed difference is an inconsistent response policy in this fictional service. It does not, by itself, demonstrate a client-side compromise. The proposed fix is to align the preview route with the agreed policy and confirm that document rendering still works. Evidence EV-04 would include sanitized headers and the configuration state of the reviewed build.

> The charts and route names on these exhibit pages were invented for this sample report.