LFMSecurity

CLIENT CONFIDENTIAL

Web Application Security Report

Acme Example Co.

ENGAGEMENT ID	SAMPLE-WEB-001
ASSESSMENT TYPE	Web Application Security
ASSESSMENT DATES	2026-05-06 to 2026-05-08
REPORT DATE	2026-05-10
PREPARED BY	LFMSecurity
CLASSIFICATION	Client Confidential

Executive Risk Snapshot

Acme Example Co. engaged LFMSecurity to perform a fixed-scope Web Application Security review. The assessment objective was to identify practical security issues within the approved scope and provide evidence-backed remediation priorities. This package is a mock sample generated from local files; no live testing is represented.

Executive Dashboard

Assessment posture, finding count, and remediation priorities.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	1	1	0	0

Priority Actions

1. Enforce server-side authorization on every object access, bind records to the requesting tenant and role, and add regression tests for horizontal and vertical
2. Add per-account and per-source throttling, normalize user-facing responses, and monitor repeated reset attempts.
3. Complete owner review and confirm remediation priorities.

Key Findings Snapshot

FW-WEB-SAMPLE-001 | High Cross-Role Account Record Access	https://app.example.invalid/accounts/{account_id}
FW-WEB-SAMPLE-002 | Medium Password Reset Flow Lacks Rate Limiting	https://app.example.invalid/reset-password

Table Of Contents

Executive Summary

Acme Example Co. engaged LFMSecurity to perform a fixed-scope Web Application Security review. The assessment objective was to identify practical security issues within the approved scope and provide evidence-backed remediation priorities. This package is a mock sample generated from local files; no live testing is represented.

The report includes 2 finding(s): High 1, Medium 1.

Key Findings

ID	SEVERITY	TITLE	AFFECTED ASSET	ASSESSMENT AREA
FW-WEB-SAMPLE-001	High	Cross-Role Account Record Access	https://app.example.invalid/accounts/{account_id}	Authorization And Data Access
FW-WEB-SAMPLE-002	Medium	Password Reset Flow Lacks Rate Limiting	https://app.example.invalid/reset-password	Application Workflow Review

Priority Actions

1. Enforce server-side authorization on every object access, bind records to the requesting tenant and role, and add regression tests for horizontal and vertical access boundaries.
2. Add per-account and per-source throttling, normalize user-facing responses, and monitor repeated reset attempts.
3. Complete owner review and confirm remediation priorities.

Scope And Objectives

Objective

Assess whether approved application workflows enforce expected authentication, authorization, data handling, and input validation controls, with emphasis on issues that could expose customer data, break tenant boundaries, or undermine core business workflows.

Scope

Anything not explicitly listed as in scope was not included in this assessment. The report is limited to the approved assets, testing windows, and test classes.

ASSET	TESTING NOTES

Application URL: https://app.example.invalid	Approved in-scope asset
Application URL: https://api.example.invalid	Approved in-scope asset

Testing Windows

WINDOW	NOTES
2026-05-06 09:00-17:00 America/New_York	Approved testing window

Methodology

Web Application Security reviews evaluate approved applications and APIs with the access level authorized for the engagement. Coverage typically includes application mapping, authentication and session behavior, role and tenant authorization, input handling, business logic, file handling, API behavior, and regression-oriented remediation guidance.

PHASE	COVERAGE
Preparation	Confirm approved URLs, roles, test accounts, workflows, exclusions, stop conditions, and data handling requirements.
Application mapping	Map reachable functionality, roles, API calls, trust boundaries, and sensitive workflows.
Control review	Review authentication, session handling, authorization, input handling, business logic, file behavior, and API controls.
Risk analysis	Rank findings by data exposure, privilege impact, workflow abuse potential, and remediation urgency.
Reporting	Document evidence-backed findings, implementation guidance, and validation criteria suitable for regression testing.

Standards And References

- OWASP Web Security Testing Guide.
- OWASP Application Security Verification Standard.
- OWASP API Security Top 10 where APIs are in scope.

Assessment Summary

Web Application Security testing identified the findings and remediation priorities below. The assessment did not expand beyond the approved assets, and evidence was limited to sanitized observations needed to support each issue.

Risk Summary

SEVERITY	COUNT
Critical	0
High	1
Medium	1
Low	0
Informational	0

Findings

Authorization And Data Access

Finding ID: FW-WEB-SAMPLE-001: Cross-Role Account Record Access

Severity: High

Affected asset: https://app.example.invalid/accounts/{account_id}

Summary

A fictional authenticated workflow allows a lower-privileged test role to view another account record by changing an identifier in the request path.

Business Impact

Cross-account access can expose customer records, create privacy obligations, and undermine customer trust even when the affected endpoint does not allow writes.

Evidence

Evidence item EV-WEB-001 contains a sanitized role matrix and redacted request/response excerpt showing expected denial for one test role and observed access for the same role. Screenshot evidence should show only test labels and authorization outcomes.

Remediation And Validation

Enforce server-side authorization on every object access, bind records to the requesting tenant and role, and add regression tests for horizontal and vertical access boundaries. Validate that lower-privileged and cross-tenant test roles receive the approved denial response while legitimate same-tenant access still works.

References

- OWASP API Security Top 10: Broken Object Level Authorization.
- OWASP ASVS access control requirements.

Application Workflow Review

Finding ID: FW-WEB-SAMPLE-002: Password Reset Flow Lacks Rate Limiting

Severity: Medium

Affected asset: https://app.example.invalid/reset-password

Summary

The fictional password reset workflow does not show a clear rate limit or throttling behavior for repeated reset requests against a test account.

Business Impact

Unthrottled reset workflows can enable account harassment, inbox flooding, and user-enumeration support when combined with other observable response differences.

Evidence

Evidence item EV-WEB-002 contains sanitized test-account timestamps and response summaries. No real user accounts, email contents, tokens, or reset links are included.

Remediation And Validation

Add per-account and per-source throttling, normalize user-facing responses, and monitor repeated reset attempts. Validate that repeated requests are delayed or blocked without disclosing account existence.

References

- OWASP Authentication Cheat Sheet.
- OWASP ASVS authentication verification requirements.

Conclusion

The highest-priority remediation work should focus on the issues listed in Priority Actions. Closing those items first will reduce the most realistic risk identified during this Web Application Security while preserving a clear path for validation.

Appendix A: Consolidated Remediations

ID	SEVERITY	REMEDIATION PRIORITY
FW-WEB-SAMPLE-001	High	Enforce server-side authorization on every object access, bind records to the requesting tenant and role, and add regression tests for
FW-WEB-SAMPLE-002	Medium	Add per-account and per-source throttling, normalize user-facing responses, and monitor repeated reset attempts.

Severity Definitions

SEVERITY	DEFINITION
Critical	Issue is likely exploitable and could cause severe business impact, broad compromise, or material data exposure.
High	Issue presents significant risk and should be prioritized quickly, especially if exposed to untrusted users or the internet.
Medium	Issue creates meaningful risk or weakens important controls, but exploitation usually requires additional conditions.
Low	Issue is a hardening gap or limited-impact weakness that should be addressed through normal remediation planning.
Informational	Observation improves security awareness, documentation, or future planning but is not currently a confirmed vulnerability.

Appendix B: Assessment Coverage

ASSESSMENT TYPE	AREAS REVIEWED	EVIDENCE STYLE
Web Application Security	https://app.example.invalid, https://api.example.invalid	Sanitized evidence excerpts and screenshot notes where relevant