LFMSecurity

CLIENT CONFIDENTIAL

External Attack Surface Report

Acme Example Co.

ENGAGEMENT ID	SAMPLE-EXT-001
ASSESSMENT TYPE	External Attack Surface
ASSESSMENT DATES	2026-05-01 to 2026-05-02
REPORT DATE	2026-05-04
PREPARED BY	LFMSecurity
CLASSIFICATION	Client Confidential

Executive Risk Snapshot

Acme Example Co. engaged LFMSecurity to perform a fixed-scope External Attack Surface 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	0	1	1	1

Priority Actions

1. Restrict administrative access behind VPN, an identity-aware access gateway, or allowlisted management networks.
2. Add a tested Content Security Policy, define frame restrictions with frame-ancestors, and validate the policy in staging before production enforcement.
3. Inventory legitimate senders, confirm SPF and DKIM alignment, monitor aggregate reports, and progress toward stricter DMARC enforcement once legitimate mail flow is

Key Findings Snapshot

FW-EXT-SAMPLE-001 | Medium Public Administrative Login Surface	https://www.example.invalid/admin
FW-EXT-SAMPLE-002 | Low Missing Browser Security Headers	https://www.example.invalid
FW-EXT-SAMPLE-003 | Informational Email Authentication Policy Observation	example.invalid

Table Of Contents

Executive Summary

Acme Example Co. engaged LFMSecurity to perform a fixed-scope External Attack Surface 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 3 finding(s): Medium 1, Low 1, Informational 1.

Key Findings

ID	SEVERITY	TITLE	AFFECTED ASSET	ASSESSMENT AREA
FW-EXT-SAMPLE-001	Medium	Public Administrative Login Surface	https://www.example.invalid/admin	Public Exposure
FW-EXT-SAMPLE-002	Low	Missing Browser Security Headers	https://www.example.invalid	Web And TLS Configuration
FW-EXT-SAMPLE-003	Informational	Email Authentication Policy Observation	example.invalid	DNS And Email Security

Priority Actions

1. Restrict administrative access behind VPN, an identity-aware access gateway, or allowlisted management networks.
2. Add a tested Content Security Policy, define frame restrictions with frame-ancestors, and validate the policy in staging before production enforcement.
3. Inventory legitimate senders, confirm SPF and DKIM alignment, monitor aggregate reports, and progress toward stricter DMARC enforcement once legitimate mail flow is validated.

Scope And Objectives

Objective

Identify internet-facing exposure that could be discovered or abused by an unauthenticated external actor, then prioritize practical reductions in exposed services, administrative access, DNS/email misconfiguration, TLS/header weaknesses, and known vulnerability indicators.

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
Domain: example.invalid	Approved in-scope asset
IP range: 203.0.113.10/32	Approved in-scope asset
Application URL: https://www.example.invalid	Approved in-scope asset

Testing Windows

WINDOW	NOTES
2026-05-01 09:00-17:00 America/New_York	Approved testing window

Methodology

External Attack Surface reviews evaluate the approved public footprint from an unauthenticated internet perspective. Coverage typically includes asset confirmation, passive discovery, safe service discovery, DNS and email security posture, TLS and HTTP configuration, exposed management surfaces, known vulnerability indicators, and unauthenticated web baseline observations.

PHASE	COVERAGE
Preparation	Confirm authorized assets, testing windows, exclusions, stop conditions, and data handling requirements.
Public footprint review	Review approved domains, IP ranges, public hostnames, certificate records, and visible service inventory.
Exposure validation	Safely validate reachable services, management surfaces, TLS posture, HTTP headers, DNS/email security records, and known vulnerability indicators.
Risk analysis	Rank findings by exposure, likelihood, exploitability, and realistic business consequence.
Reporting	Document evidence-backed findings, prioritized remediations, and validation criteria.

Standards And References

- CIS Controls for asset inventory, secure configuration, vulnerability management, and access control.
- OWASP guidance where exposed web surfaces are included in scope.
- Current vendor hardening and lifecycle guidance where technology is identified.

Assessment Summary

External Attack Surface 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	0
Medium	1
Low	1
Informational	1

Findings

Public Exposure

Finding ID: FW-EXT-SAMPLE-001: Public Administrative Login Surface

Severity: Medium

Affected asset: https://www.example.invalid/admin

Summary

A fictional administrative login path is documented as publicly reachable from the internet. No login attempts, password attacks, or exploit validation are represented in this sample.

Business Impact

Public administrative interfaces give attackers a focused target for credential attacks, vulnerability research, and future exploitation if credentials or software weaknesses are

introduced.

Evidence

Evidence item EV-EXT-001 contains a sanitized local-only page title excerpt and a screenshot note for the visible login form. The sample does not include credentials, cookies, or real customer data.

Remediation And Validation

Restrict administrative access behind VPN, an identity-aware access gateway, or allowlisted management networks. Enforce MFA for all administrative users and validate from an untrusted network that the admin interface is no longer directly reachable.

References

- OWASP Authentication Cheat Sheet.
- CIS Controls access control guidance.

Web And TLS Configuration

Finding ID: FW-EXT-SAMPLE-002: Missing Browser Security Headers

Severity: Low

Affected asset: https://www.example.invalid

Summary

The fictional public web surface is missing browser hardening headers that help limit the impact of content injection, clickjacking, and mixed-content mistakes.

Business Impact

Missing headers are usually hardening gaps, but they can increase the impact of a separate web vulnerability by allowing unsafe framing, script execution, or insecure browser behavior.

Evidence

Evidence item EV-EXT-002 contains a sanitized header review excerpt listing the missing controls. A screenshot is only useful if it shows an affected browser behavior without exposing user data.

Remediation And Validation

Add a tested Content Security Policy, define frame restrictions with frame-ancestors, and validate the policy in staging before production enforcement. Confirm the expected headers are present and legitimate application behavior still works.

References

- OWASP Secure Headers Project.
- MDN Content Security Policy documentation.

DNS And Email Security

Finding ID: FW-EXT-SAMPLE-003: Email Authentication Policy Observation

Severity: Informational

Affected asset: example.invalid

Summary

The fictional domain has an email authentication posture that should be staged before moving to stricter enforcement.

Business Impact

Weak or incomplete email authentication can make spoofing harder to investigate and may reduce confidence in mail claiming to come from the organization.

Evidence

Evidence item EV-EXT-003 contains a sanitized DNS record excerpt for SPF, DKIM, and DMARC alignment review.

Remediation And Validation

Inventory legitimate senders, confirm SPF and DKIM alignment, monitor aggregate reports, and progress toward stricter DMARC enforcement once legitimate mail flow is validated.

References

- DMARC.org overview guidance.
- CISA email authentication guidance.

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 External Attack Surface while preserving a clear path for validation.

Appendix A: Consolidated Remediations

ID	SEVERITY	REMEDIATION PRIORITY
FW-EXT-SAMPLE-001	Medium	Restrict administrative access behind VPN, an identity-aware access gateway, or allowlisted management networks.

FW-EXT-SAMPLE-002	Low	Add a tested Content Security Policy, define frame restrictions with frame-ancestors, and validate the policy in staging before
FW-EXT-SAMPLE-003	Informational	Inventory legitimate senders, confirm SPF and DKIM alignment, monitor aggregate reports, and progress toward stricter DMARC enforcement once legitimate mail

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
External Attack Surface	example.invalid, 203.0.113.10/32, https://www.example.invalid	Sanitized evidence excerpts and screenshot notes where relevant