Sample Security Audit Report

Assessment type: Illustrative web application security review
Prepared for: Fictional Example Organization
Report status: Sample document — not an assessment of a real system

> **Important:** This sample uses a fictional environment and illustrative findings. It is provided to demonstrate report structure only; it does not represent testing performed for a client or a guarantee of security.

1. Executive summary

This example review demonstrates how security observations can be prioritized and communicated with practical remediation guidance. The fictional application is assumed to be a small customer portal. No live systems were accessed, scanned, or tested in preparing this sample.

> **Illustrative outcome:** Two sample observations are shown below: one medium-priority configuration issue and one low-priority information disclosure concern. These are examples only and must not be interpreted as verified vulnerabilities.

2. Sample scope and approach

Item	Illustrative scope
Application	Fictional customer portal (example.invalid)
Review areas	Transport and browser security configuration; error handling
Excluded	Production systems, denial-of-service testing, social engineering, and third-party infrastructure
Method	Example documentation and configuration review workflow; no tests were executed

3. Illustrative findings

ID	Example observation	Severity	Status
SAMPLE-01	Recommended browser security headers are not configured	Medium	Illustrative only
SAMPLE-02	Error responses may reveal implementation details	Low	Illustrative only

4. Finding details

SAMPLE-01 — Recommended browser security headers

Severity: Medium (example) **Confidence:** Not assessed

Example impact: Missing browser security controls can reduce defense-in-depth and may increase the impact of other application weaknesses.

Recommendation: Review the application's browser-facing routes and configure appropriate headers—such as Content-Security-Policy, X-Content-Type-Options, and Referrer-Policy—based on application behavior. Test policies in a staging environment before enforcing them.

SAMPLE-02 — Detailed error responses

Severity: Low (example) **Confidence:** Not assessed

Example impact: Detailed errors can disclose framework, path, or implementation information that is not needed by end users.

Recommendation: Return generic error messages to users, keep diagnostic details in access-controlled server logs, and ensure sensitive data is excluded from logs.

5. Prioritized remediation plan

1. Review and test suitable browser security headers in a non-production environment.
2. Standardize user-facing error responses and validate logging access controls.
3. Reassess configuration changes and document any accepted residual risk.

6. Limitations and responsible use

This sample is educational and illustrative. Severity labels and observations are hypothetical, not verified

against a target. A real security assessment requires written authorization, an agreed scope, evidence collection, and validation with the system owner. This document should not be used as evidence of certification, compliance, or completed testing.