PENETRATION TEST REPORT

Web Application Penetration Test Report

CLIENT	Acme Bank
ENGAGEMENT ID	demo-web
TESTER	Komal Prasad
TARGET	https://online.acmebank.example
START DATE	2026-08-03
END DATE	2026-08-06
MODULE	Web Application Pentest
OWASP FRAMEWORK	OWASP Top 10 — 2021

CRITICAL 1 HIGH 1 LOW 1

Table of Contents

1. Executive Summary

During the engagement, a total of **3** findings were identified against https://online.acmebank.example: 1 critical, 1 high and 1 low.

The most significant issue is **SQL Injection in login parameter** (Critical, CVSS 9.8), which should be remediated as a priority.

The overall risk to the application is assessed as **Critical**. Immediate remediation is strongly recommended before the application is exposed to untrusted users.

Detailed technical findings, evidence, and remediation guidance are provided in the following sections. All testing was performed with appropriate authorization.

Severity Breakdown

Severity	Count	CVSS Range
Critical	1	9.0 – 10.0
High	1	7.0 – 8.9
Medium	0	4.0 – 6.9
Low	1	0.1 – 3.9
Info	0	0.0
TOTAL	**3**	

2. Engagement Overview

Client	Acme Bank
Engagement ID	demo-web
Tester	Komal Prasad
Start Date	2026-08-03
End Date	2026-08-06
Target	https://online.acmebank.example
Module	Web Application Pentest
OWASP Framework	OWASP Top 10 — 2021

3. Scope & Methodology

In-Scope

- https://online.acmebank.example
- https://online.acmebank.example/docs/
- https://online.acmebank.example/api/

Out of Scope

- https://online.acmebank.example/admin-panel/

Testing Checklist

Step	Status
Reconnaissance & scope confirmation	Complete
Information gathering & technology fingerprinting	Complete
Configuration & deployment review	Complete
Authentication & session management testing	Complete
Authorization / access control testing	Complete
Input validation & injection testing (SQLi, XSS, SSTI, CMDi, ...)	Complete
CSRF / CORS / clickjacking / security headers	Complete
File upload & download handling	Complete
Business logic & abuse-case testing	Pending
Error handling & information disclosure	Pending
Client-side / supply-chain review (third-party JS, dependencies)	Pending
Retesting of confirmed findings	Pending

4. Findings Summary

ID	Title	Severity	CVSS	Status
F-001	SQL Injection in login parameter	Critical	9.8	open
F-002	Broken Access Control — IDOR on account statements	High	6.5	open
F-003	Security headers missing (CSP, HSTS, X-Frame-Options)	Low	4.3	open

5. Detailed Findings

F-001 — SQL Injection in login parameter [Critical]

Category	A03:2021 — Injection
Severity	Critical
CVSS v3.1	9.8 · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Status	open
Affected URL	https://online.acmebank.example/login
Parameter(s)	username
HTTP Method	POST

DESCRIPTION

The username parameter of the login form is concatenated directly into a SQL query, allowing authentication bypass and full database extraction.

EVIDENCE / PROOF OF CONCEPT

POST /login HTTP/1.1\nusername=' OR '1'='1'--&password=x\nHTTP/1.1 302 Found\nLocation: /dashboard

IMPACT

Full authentication bypass, complete disclosure of customer records, funds manipulation.

REMEDIATION

Use parameterized queries / prepared statements everywhere; validate input; apply least-privilege DB accounts.

REFERENCES

- https://owasp.org/Top10/A03_2021-Injection/

F-002 — Broken Access Control — IDOR on account statements [High]

Category	A01:2021 — Broken Access Control
Severity	High
CVSS v3.1	6.5 · CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Status	open
Affected URL	https://online.acmebank.example/statements
Parameter(s)	account
HTTP Method	GET

DESCRIPTION

Account statement endpoint trusts a user-supplied account number without verifying ownership, exposing other customers' statements.

EVIDENCE / PROOF OF CONCEPT

GET /statements?account=4102937 with a session for account 4102936 returned full statements.

IMPACT

Cross-account data exposure — sensitive financial records of any customer.

REMEDIATION

Enforce server-side object-level authorization on every resource access.

F-003 — Security headers missing (CSP, HSTS, X-Frame-Options) [Low]

Category	A05:2021 — Security Misconfiguration
Severity	Low
CVSS v3.1	4.3 · CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
Status	open
Affected URL	https://online.acmebank.example/
HTTP Method	GET

DESCRIPTION

No Content-Security-Policy, HSTS, or X-Frame-Options headers observed on any response.

EVIDENCE / PROOF OF CONCEPT

curl -sI https://online.acmebank.example/ — no security headers present.

IMPACT

Increases the risk and impact of XSS, clickjacking, and protocol-downgrade attacks.

REMEDIATION

Set a strict CSP, HSTS (with preload), X-Frame-Options: DENY, and Referrer-Policy.

6. Conclusion & Recommendations

The engagement identified 3 finding(s). All findings should be tracked to closure with defined owners and target dates. High and critical findings should be remediated before the application is exposed to untrusted users. A retest should be scheduled once fixes are deployed.

Remediation Priority

Severity	Recommended Timeline
Critical	Immediate (within days)
High	Short term (within 2 weeks)
Medium	Near term (next release)
Low	Scheduled (next cycle)
Info	Informational

Appendix A — OWASP Category Reference

OWASP Top 10 — 2021

Code	Category
A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A10:2021	Server-Side Request Forgery (SSRF)