Umbra

SAMPLE — Acme Bank external penetration test

Executive Summary

Prepared for	ACME Bank
Date	2026-11-06
Classification	Confidential

Risk Overview

Overall risk: Critical · Total findings: 19 · Confirmed: 6

Severity	Findings
Critical	3
High	4
Medium	6
Low	4
Info	2
Unclassified	0

Summary

External infrastructure and web application assessment of internet-facing banking services.

Key findings

• Remote code execution in Apache Struts (S2-066): The application runs outdated software with publicly known security flaws.

• SQL injection in /api/accounts/search: An attacker on the internet can read or change the application's database, including customer data.

• Broken access control: view any customer's statements: Any customer can view other customers' private records by changing a number in the request.

• Outdated OpenSSH with known vulnerabilities: Several systems are missing security updates for flaws that attackers actively exploit.

• Stored cross-site scripting in support tickets: A user can plant code that runs in the browsers of other users, including administrators.

Engagement scope

Client: ACME Bank

Testing period: –

In scope	Engagement type
netbanking.acme-bank.example	domain
loans.acme-bank.example	domain
10.20.0.0/24	cidr

Out of scope	Engagement type
10.20.9.0/24	cidr

Methodology coverage

Checklist	Tested	Passed	Failed	%
OWASP Top 10 (2021)	7/24	4	3	29

Findings summary

#	Name	Severity	Status	Affected asset
1	Remote code execution in Apache Struts (S2-066)	Critical	Open	10.20.0.21
2	SQL injection in /api/accounts/search	Critical	Open	10.20.0.10
3	SQL injection in login form	Critical	Open	10.20.0.10
4	Broken access control: view any customer's statements	High	Open	10.20.0.10
5	Outdated OpenSSH	High	Closed	10.20.0.5
6	Outdated OpenSSH with known vulnerabilities	High	Open	10.20.0.5
7	Stored cross-site scripting in support tickets	High	Open	10.20.0.10
8	Exposed Jenkins dashboard	Medium	Open	10.20.1.40
9	Missing HTTP security headers	Medium	Closed	10.20.0.30
10	SMB signing not required	Medium	Open	10.20.2.15
11	User enumeration on login page	Medium	Open	10.20.0.10
12	Weak password policy	Medium	Open	10.20.0.10
13	Weak TLS configuration (TLS 1.0/1.1 enabled)	Medium	Open	10.20.0.30
14	Cookie without Secure flag	Low	Closed	10.20.0.30
15	Directory listing enabled	Low	Open	portal.acme.example
16	Directory listing enabled on /static	Low	Open	10.20.0.30
17	Verbose error messages disclose stack traces	Low	Open	10.20.0.21
18	Open port 3389 (RDP) on jump host	Info	Open	10.20.2.15
19	Server version disclosure	Info	Open	10.20.0.5