

Acme Financial Services

Scheduled Security Testing - Q4 2024

CONFIDENTIAL - INTERNAL USE ONLY

Overview

This document outlines scheduled penetration testing and security assessments for Q4 2024.

Prepared by: Security Operations Team

Date: October 1, 2024

Next Review: January 1, 2025

Scheduled Tests

Test 1: Automated Vulnerability Scanning

Type: Weekly Automated Scan

Schedule: Every Tuesday, 01:30 AM PST

Target: All production systems

Tool: Internal Security Scanner (Python-based)

Source IP: 192.168.1.100 (Internal Network)

Scope:

- API endpoints
- Web applications
- Mobile app backends
- Authentication services

Expected Activity:

- Failed login attempts (testing auth)
- Sequential endpoint probing
- Port scanning

- SSL/TLS validation

Test Accounts:

- Account IDs: 5001-5010 (Test range)
- User: `sec_team`
- IP Range: 10.0.0.0/24

Status:  Active

Test 2: Quarterly Penetration Test

Type: Manual Penetration Test

Schedule: October 20-25, 2024

Vendor: External Security Firm (CyberSec Partners)

Contact: pentesting@cybersecpartners.com

Scope:

- Web application security (OWASP Top 10)
- API security testing
- Network infrastructure
- Social engineering (email phishing simulation)

Approved Source IPs:

- 203.0.113.0/24 (Testing range)
- To be confirmed 48 hours before test

Status:  Upcoming

Test 3: Compliance Audit

Type: SOC 2 Type II Audit

Schedule: November 15-30, 2024

Auditor: PriceWaterhouse Coopers (PwC)

Focus: Security controls, access management, logging

Status:  Scheduled

Important Notes

For Security Operations:

- Do NOT block test traffic from scheduled IPs
- Monitor tests but do NOT interfere
- Document any anomalies or false positives
- Review alerts after each test cycle

For Development Teams:

- Weekly scans may trigger alerts
- Test accounts (5001-5010) are exempt from rate limits
- Expect 401 errors during auth testing (expected behavior)

For SOC Team:

- Tune SIEM rules to reduce false positives
 - All scheduled tests are logged in ticketing system
 - Escalate only if activity outside scheduled windows
-

Test Account Credentials

Test Accounts: 5001-5010

Purpose: Security testing only

Access: Security team and authorized vendors

Characteristics:

- No real customer data
 - Isolated from production database
 - Flagged in monitoring systems
-

Emergency Contacts

Security Team Lead: security-lead@acme.com

SOC Manager: soc-manager@acme.com

On-Call Engineer: +1-555-123-4567

Revision History

Version	Date	Changes	Author
1.0	2024-10-01	Initial schedule	Security Team
1.1	2024-10-05	Added test account range	Security Team

This document is confidential and intended for internal use only.