WHITE PAPER

Top Compliance and Penetration Testing Finds

What To Do Next

The most common vulnerabilities identified across web application, network, and compliance assessments — with concrete remediation steps to address each category.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

A consistent set of vulnerabilities recurs across penetration testing and compliance assessments regardless of industry, size, or technology stack. Understanding these patterns allows security leaders to prioritize controls that deliver the greatest risk reduction per dollar invested.

AUTH & ACCESS

2. Authentication and Access Control Findings

Finding	Description	Remediation
Weak / Default Credentials	Default credentials on network devices, admin consoles, and third-party integrations.	Enumerate all devices for defaults during onboarding. Enforce unique, complex credentials and a rotation policy.
Missing MFA	MFA absent on VPN, remote access, email, and cloud portals. Single-factor auth is the leading enabler of account compromise.	Enforce MFA on all remote and privileged access. Prioritize phishing-resistant FIDO2/WebAuthn for admin accounts.
Excessive Privilege	Users and service accounts granted more access than required. Admin accounts used for daily tasks.	Implement least privilege. Audit permissions quarterly. Separate admin from daily-use accounts.
IDOR (Broken Object Auth)	API endpoints fail to verify the authenticated user is authorized for the requested resource.	Implement object-level authorization on every API endpoint. Validate resource ownership server-side.

NETWORK

3. Network Security Findings

Finding	Description	Remediation
Unpatched Systems	Critical and high CVEs on internet-facing systems and network devices. Patch cycles exceeding 30 days.	Implement vulnerability management with SLAs: critical ≤15 days, high ≤30 days. Use automated scanning.
Permissive Firewall Rules	Broad rules between network segments. Legacy rules for decommissioned systems.	Audit rules annually. Remove unused rules. Implement zero-trust segmentation between sensitive environments.
Insecure TLS Config	Deprecated protocols (TLS 1.0/1.1/SSL), weak ciphers, expired certs, and missing HSTS.	Enforce TLS 1.2 minimum (1.3 preferred). Disable weak ciphers. Automate certificate renewal. Enable HSTS.

Finding	Description	Remediation
Exposed Management Interfaces	RDP, SSH, and admin panels directly accessible from the internet without VPN or MFA.	Remove all management interface internet exposure. Route admin access through VPN or zero-trust with MFA.

APPLICATION

4. Application Security Findings

Finding	Description	Remediation
Injection (SQLi/XXE/SSTI)	User input passed unsanitized to database queries, XML parsers, and template engines.	Parameterize all queries. Disable external entity processing. Use sandboxed templates. Add SAST to CI/CD.
Cross-Site Scripting (XSS)	Reflected, stored, and DOM-based XSS enabling session hijacking and credential theft.	Implement strict output encoding. Deploy Content Security Policy. Use frameworks with built-in XSS protections.
Broken API Authentication	API endpoints missing auth, accepting expired tokens, or with flawed JWT implementation.	Authenticate every endpoint. Validate JWT signatures, algorithms, and claims. Implement token expiry and rotation.
Sensitive Data Exposure	PII, API keys, and credentials returned in API responses or logged in plaintext.	Audit response bodies for over-exposure. Scan repos for secrets. Encrypt sensitive data at rest and in transit.

DATA & COMPLIANCE

5. Data Security and Compliance Gaps

Finding	Description	Remediation
Unencrypted Data at Rest	Databases and backups containing PII, PHI, or cardholder data stored without encryption.	Implement AES-256 for all sensitive data at rest. Enforce encryption on backup media. Migrate from MD5/SHA-1.
Cloud Storage Misconfiguration	S3 buckets or Azure Blob containers publicly accessible due to misconfigured ACLs.	Enable Block Public Access at account level. Use policy guardrails to prevent public bucket creation. Use CSPM.
Insufficient Logging	Missing logs for authentication and administrative events; no alerting on critical security events.	Centralize logging for all auth, authorization, and privileged events. Set alert thresholds. Retain logs 12+ months.

Finding	Description	Remediation
Untested Incident Response	IR plans exist on paper but have not been exercised. Key roles and escalation paths undefined.	Conduct annual tabletop exercises. Document escalation paths and external contacts. Test backup restoration.

PRIORITIZATION

6. Prioritizing Remediation

- Critical: Address immediately — these are direct paths to data breach or full system compromise.
- High: Remediate within 30 days — significant risk but typically requires additional attacker conditions.
- Medium: Schedule within 90 days — contributes to attacker dwell time and lateral movement.
- Low/Informational: Log and address during scheduled hardening cycles.
- Validate all fixes: Request retesting for Critical and High findings to confirm effectiveness.

How Lorikeet Security Helps

Lorikeet Security provides penetration testing, compliance assessments, and remediation consultation. Every engagement includes an attestation letter and free retest within 30 days. Contact us at lorikeetsecurity.com or call (689) 202-3940.