Sample Pentest Report · Sanitized

Prepared by Axel Uriel Gutiérrez Maya / Clest · Demonstration artifact for recruiter and technical review. No real client data included.

Executive Summary

The assessment identified weaknesses in authentication, input validation and Active Directory hygiene. The most relevant risks were credential exposure, insufficient access control and exploitable service configuration. Recommended remediation focuses on privilege reduction, secure configuration, patching and stronger monitoring.

Sample Finding 1 · Exposed Credentials in SYSVOL/GPP

Severity	High
Category	Active Directory Security
Impact	Credential disclosure can enable initial domain access and lateral movement.
Evidence	SMB enumeration exposed policy XML containing encrypted credential material.
Recommendation	Remove legacy GPP credentials, rotate affected accounts, audit SYSVOL, enforce least privilege

Sample Finding 2 · UNION-based SQL Injection

• Risk: database content exposure through unsafe query construction and insufficient input handling.

• Validation: column count enumeration followed by controlled UNION payload to demonstrate retrieval of multiple values in one column.

• Recommendation: parameterized queries, server-side validation, least-privilege DB accounts, error handling and regression testing.

Delivery Style

Reports are structured with business impact, technical evidence, reproducible steps, affected assets, severity rationale, remediation actions and retest criteria.