Cloud Storage Penetration Testing Report

Date: [Insert Date]

Client: [Client Name/Organization]

Tested By: [Pentester Name/Team]

1. Executive Summary

This report describes the findings from the penetration testing of the client's cloud storage environment, outlining key risks, discovered vulnerabilities, and overall security posture.

2. Scope

- Cloud Storage Platform: [e.g., AWS S3, Azure Blob, Google Cloud Storage]
- Tested Resources: [List Buckets/Containers & Folders]
- Testing Period: [Start Date] to [End Date]

3. Methodology

1. Review of access control configurations
2. Enumeration of storage buckets/containers
3. Testing for public access/misconfigurations
4. Assessment of encryption at rest and in transit
5. Discovery of credentials/secrets
6. Privilege escalation attempts

4. Findings Summary

ID	Risk	Description	Severity	Status
F-001	Publicly Accessible Bucket	One storage bucket was found accessible without authentication.	High	Unresolved
F-002	Weak Access Controls	Write permissions overexposed to multiple users/groups.	Medium	Unresolved
F-003	Unencrypted Data	Data-at-rest encryption was not enabled for several objects.	Low	Unresolved

5. Detailed Findings & Recommendations

5.1 Publicly Accessible Bucket (F-001)

Risk: Unauthorized data exposure.

Recommendation: Restrict bucket access policies; ensure only authorized users can access.

5.2 Weak Access Controls (F-002)

Risk: Potential data manipulation by unauthorized users.

Recommendation: Review and revise permissions; follow the principle of least privilege.

5.3 Unencrypted Data (F-003)

Risk: Increased risk of data breach if storage is compromised.

Recommendation: Enable default encryption for all buckets and stored objects.

6. Conclusion

The penetration test identified key misconfigurations in the cloud storage setup, primarily relating to public accessibility, access control, and data encryption. Addressing these issues is critical to reducing the attack surface and safeguarding sensitive data.

7. Appendix

- References to best practices (e.g.,