Vulnerability Assessment & Penetration Testing (VAPT) Report

Prepared by: RedOps Cyber Intelligence Group

Date: April 17, 2025

1. Executive Summary

This report provides a sanitized summary of a recent Vulnerability Assessment and Penetration Test conducted by RedOps Cyber Intelligence Group. The purpose of the engagement was to identify vulnerabilities in the client's internal and external environments and recommend corrective actions.

2. Methodology

The assessment followed a hybrid black-box and gray-box methodology, leveraging industry-standard frameworks including OWASP, PTES, and NIST SP 800-115. Tools used included Nmap, Burp Suite, and custom recon scripts.

3. Key Findings

- Finding 1: Outdated Apache Server (CVE-2021-41773)
  Impact: High | Affects: Web server | Exploitable via crafted requests
- Finding 2: IDOR Vulnerability in /api/user endpoint
  Impact: Medium | Affects: API | Allows privilege escalation
- Finding 3: S3 Bucket Misconfigured (Public Read)

Impact: Medium | Affects: Cloud Storage | Risk of data leakage

4. Recommendations

- Patch all publicly exposed services.

- Implement role-based access controls.

- Enable logging and alerting on critical infrastructure.

- Conduct monthly vulnerability scans and penetration tests.

Contact & Attribution

RedOps Cyber Intelligence Group

Contact: sam@redopscyber.com | www.redopscyber.com