IoT Device Penetration Testing Findings Report

1. Executive Summary

This report summarizes the key findings from the penetration testing of the IoT device: **Sample Device XYZ**. The assessment was conducted to evaluate the security posture of the device and identify potential vulnerabilities that may be exploited by malicious actors.

2. Scope

- Physical device: Sample Device XYZ (FW v1.2.3)
- Web management interface (HTTP, HTTPS)
- Mobile application (Android/iOS, v2.1.0)
- Cloud API endpoints

3. Methodology

- Reconnaissance and Attack Surface Analysis
- Vulnerability Scanning and Manual Analysis
- Exploitation Attempts
- Review of Authentication, Encryption, and Data Protection Mechanisms

4. Summary of Findings

ID	Title	Severity	Status
F-01	Default Credentials Enabled	**High**	Unresolved
F-02	Insecure HTTP Communication	**Medium**	Unresolved
F-03	Information Leakage via API	**Low**	Resolved

5. Detailed Findings

F-01: Default Credentials Enabled

- **Description:** The device was shipped with factory default credentials (admin/admin), which were not enforced to be changed upon initial setup.
- **Impact:** Unauthenticated attackers could gain full control of the device.
- **Recommendation:** Require users to change credentials at first use and implement account lockout mechanisms.
- **Severity: High**
- **Status:** Unresolved

F-02: Insecure HTTP Communication

- **Description:** The web management interface supports HTTP without redirecting traffic to HTTPS.
- **Impact:** Credentials and sensitive data can be intercepted via network sniffing.
- **Recommendation:** Enforce HTTPS and disable plain HTTP access.

- **Severity: Medium**
- **Status:** Unresolved

F-03: Information Leakage via API

- **Description:** The API endpoint `/api/status` exposed device information without authentication.
- **Impact:** Could aid attackers in crafting targeted attacks.
- **Recommendation:** Require authentication for all sensitive API endpoints.
- **Severity: Low**
- **Status:** Resolved

6. Conclusion

The assessment identified several vulnerabilities, the most critical of which is the use of default credentials. Addressing these findings will significantly improve the security of the Sample Device XYZ.