2. Title: Unveiling Vulnerabilities in Google-Approved Apps

Case Story:

In today's digital-first India, apps such as DigiLocker, CoWIN, mParivahan, UMANG, eShram, ABHA, and DigiYatra form the backbone of governance and citizen services. They store sensitive information, ID proofs, medical records, vaccination details, and financial data.

Google Play Protect claims to block 1.43 million policy-violating apps in 2023 alone. Yet, research (Trend Micro, 2022) shows that 36% of apps on Google Play with over 100,000 downloads had at least one security flaw. Even Google-approved apps can have:

1. Data leaks exposing Aadhaar/PAN or health records.

2. Malware injection via third-party SDKs.

3. Permissions misuse—apps requesting more data than required.

4. Functional flaws that can be exploited for phishing or fraud.

Imagine a user downloading a government service app, trusting it because it's on the Play Store. Weeks later, their Aadhaar details are leaked due to a vulnerability in that very app. This is not hypothetical; such breaches have already occurred globally, shaking user trust.

Core Challenge:

Develop a "Security-First Framework" or prototype for a hypothetical government app (e.g., health records, ID verification, or citizen services) that prevents:

1. Data leaks (Aadhaar/PAN, health info, financial data).

2. Malware injection or third-party SDK abuse.

3. Permission misuse (location, contacts, camera).

4. Exploitable functional flaws.

Deliverables:

1. Technical Report (3–5 pages): Clear documentation of vulnerabilities found in different aops, categorised by severity (critical/high/medium/low).

2. Demo Video (2–3 mins): Show how at least one discovered issue can be demonstrated safely (without harming real users).

3. Tool/Scripts: If possible, basic tools or scripts used for vulnerability testing.

4. Prototype