Bug Bounty & Penetration Testing: Login Flaws

Default or Common Passwords

Default or Common Passwords are critical vulnerabilities often found in misconfigured applications. They include:

1. Default Credentials for Admin Panels:
   - Test /admin, /phpmyadmin using admin:admin, root:root, etc.
   - Tools: Hydra, Burp Intruder, Nuclei
   - Impact: Admin panel takeover

2. Default Passwords for IoT or Third-Party Apps:
   - Example: Jenkins (admin:admin), cameras (admin:1234)

3. Weak/Common Passwords at Registration:
   - Test for weak password acceptance: "password", "123456"

4. Shared Passwords Across Privileged Accounts:
   - Register normal account, test same password for admin users

5. Authentication Bypass via Default Tokens/API Keys:
   - Try Bearer test123 or similar headers for access

Token Leakage (JWT in URLs)

Bug Bounty & Penetration Testing: Login Flaws

Token Leakage occurs when tokens are exposed via URL, JavaScript, logs, etc.

1. JWT in URL Parameters:

   - Example: /reset?token=JWT

   - Risk: Exposed in browser history, logs

2. JWT in Referer Headers:

   - Third-party scripts can read Referer headers with tokens

3. JWT in JS/HTML:

   - Exposed in source code or network responses

4. JWT in Logs:

   - Public log files containing tokens

5. Token Reuse Without Rotation:

   - Token still valid after logout

6. JWT Without Expiry or Weak Signing:

   - Test 'alg: none' or missing 'exp' fields

   - Decode at jwt.io