CVSS Challenge Worksheet

📋 Scenario

- In today's exercise, you will be a member of the Product Security Incident Response Team (PSIRT) for "JonDale Innovations." JonDale Innovations is a technology company that develops and manages smart Internet of Things (IoT) devices for homes and businesses. The product examples today will be:
  - **JonDale HomeHub** - A central device for smart homes
  - **JonDale SmartCam** - A smart camera device
- Today's scenarios will revolve around vulnerabilities in the JonDale Innovations firmware and mobile applications, and the security of customer data related to those devices. Since this company deals with connected hardware and software that interacts with the physical world and often handles sensitive user data, their cybersecurity posture is incredibly important. A breach could have physical safety, privacy, and financial implications for their customers.
- You will be given 3 vulnerability scenarios below (CVEs). Each CVE will have a concise and clear description of the flaw, providing enough detail to pick the CVSS metrics. Your task, as a team, will be to go to the CVSS 3.1 Calculator (URL will be provided). Read the description of the CVE carefully and select the appropriate metric values (Attack Vector, Privileges Required, Impact, etc.) You will then write down the Base Score from the calculator on this sheet. That will be your flag!

CVE Example 1: "The Login Bypass"

📋 Scenario

- **CVE ID**: CVE-202X-111111
- **Vulnerability Description**: "A flaw exists in the authentication logic of the 'JonDale HomeHub' device's web management interface. An attacker on the ***same local network*** (e.g., your Wi-Fi) can bypass the login page and gain ***low-level administrative privileges*** without providing a password. This does ***not*** require user interaction. The attacker can then view device settings, modify some settings, but cannot cause a denial of service."
- **CVSS Values Chosen**
  - AV: ___, AC: ___,PR: ___,UI: ___,S: ___,C: ___,I: ___,A: ___,
- **Final Base Score**: _____

CVE Example 2: “The Remote Takeover”

📋 Scenario

- **CVE ID**: CVE-202X-2222
- **Vulnerability Description**: "A critical flaw in the 'JonDale SmartCam' allows an unauthenticated attacker on the internet to remotely execute malicious code on the device. This requires no user interaction. If exploited, the attacker gains full control of the device and can potentially access the home network.
- **CVSS Values Chosen**
    - AV: ___, AC: ___,PR: ___,UI: ___,S: ___,C: ___,I: ___,A: ___,
- **Final Base Score**: _____

CVE Example 3: “The Data Leak”

📋 Scenario

- **CVE ID**: CVE-202X-2222
- **Vulnerability Description**: "A vulnerability in the 'JonDale App' (mobile application) allows an authenticated user to view other users' non-sensitive profile information (e.g., public username, favorite color) if they know their user ID. This occurs due to improper data validation. No sensitive data like passwords or payment info is exposed. No user interaction is required from the victim.”
- **CVSS Values Chosen**
    - AV: ___, AC: ___,PR: ___,UI: ___,S: ___,C: ___,I: ___,A: ___,
- **Final Base Score**: _____