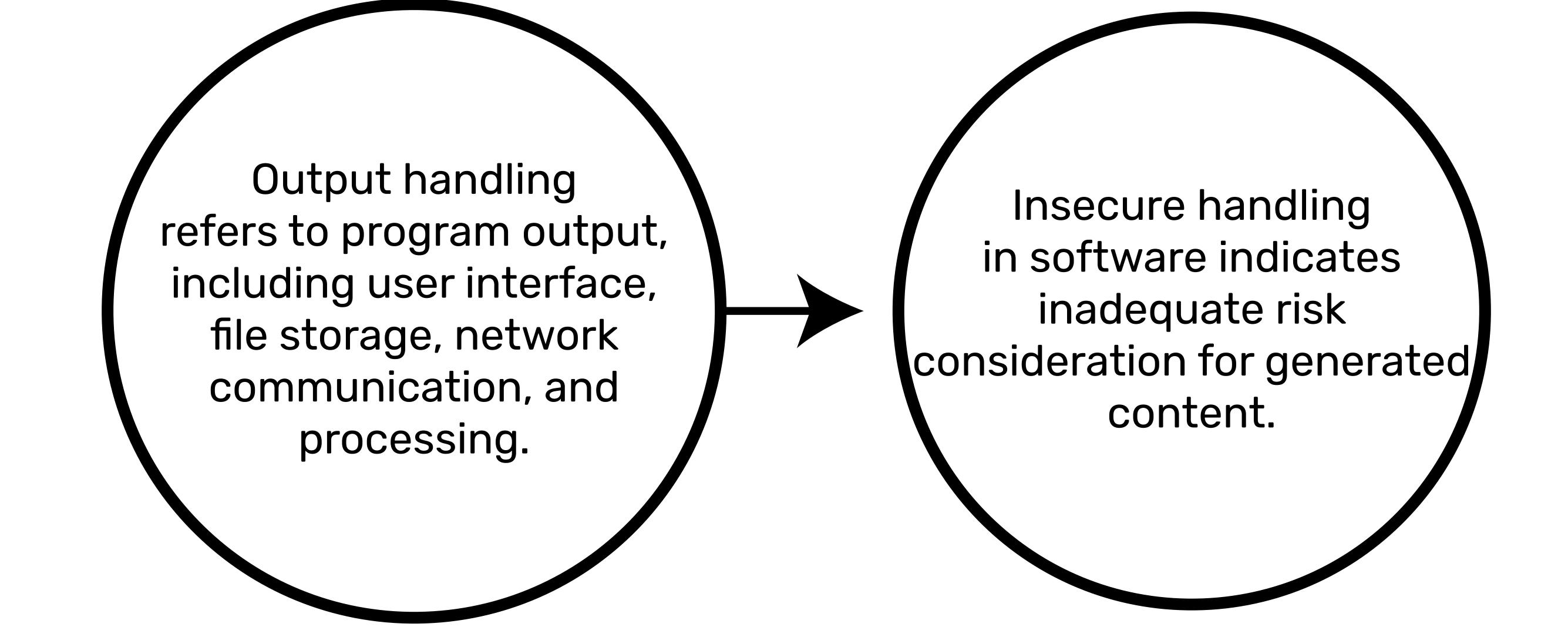
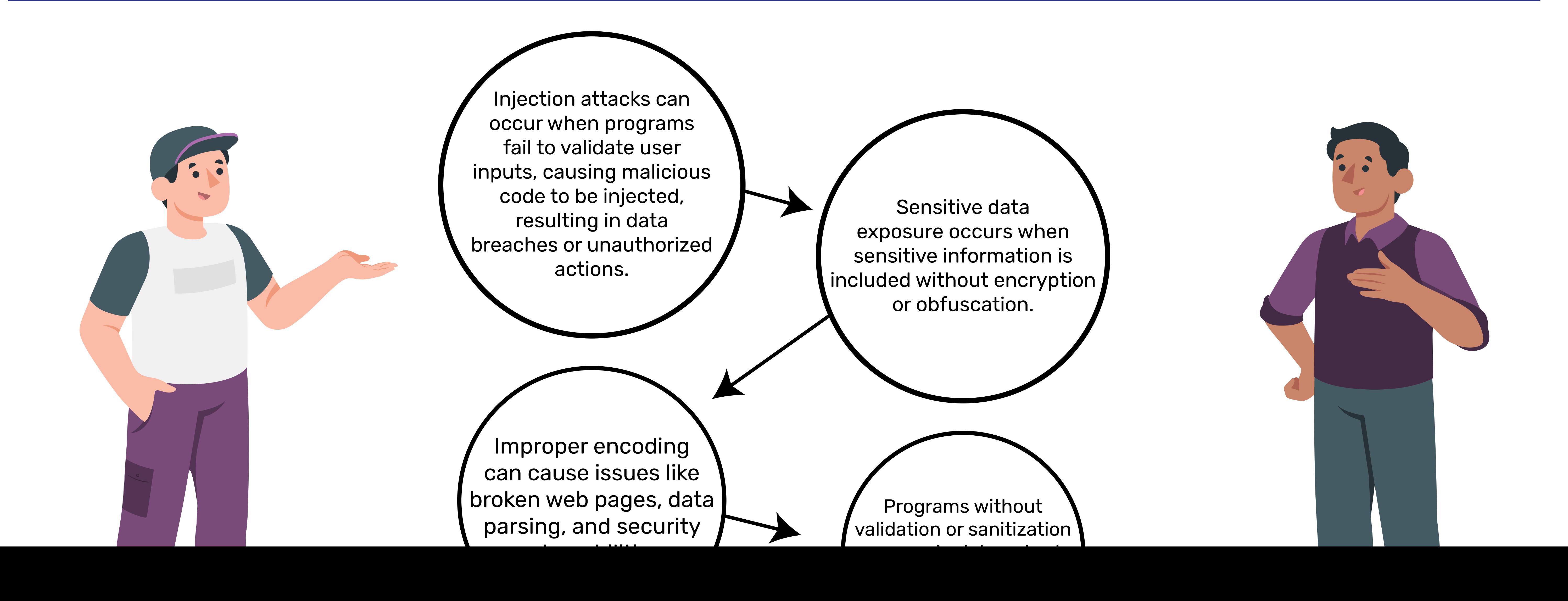


## Owasp Top 10 LLM 02: Insecure Output Handling

What Is Insecure Output Handling?

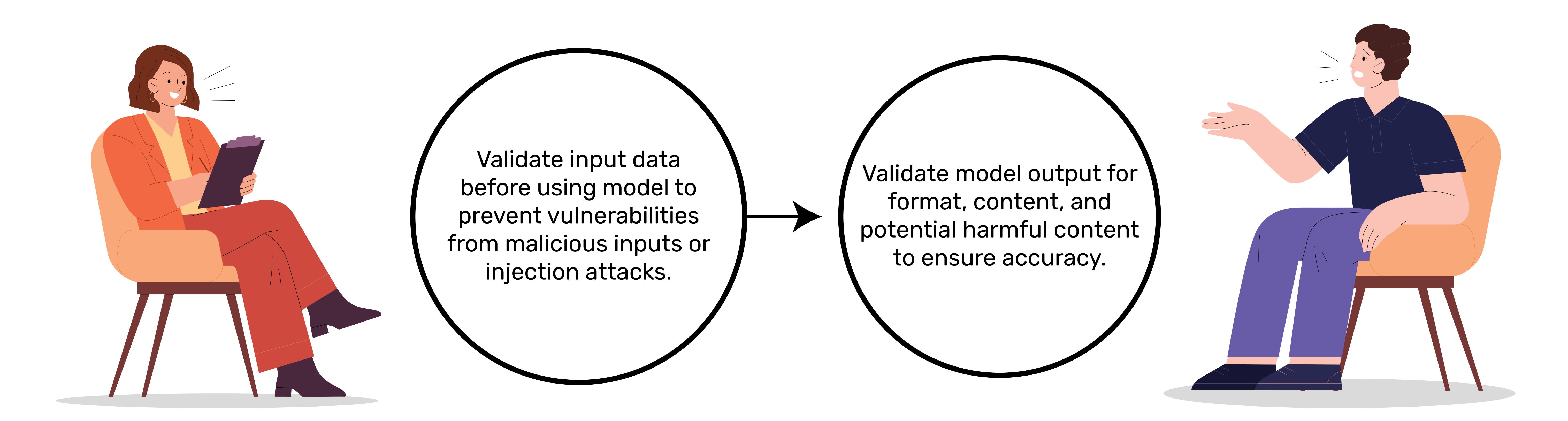


### Insecure output handling can manifest in various ways:

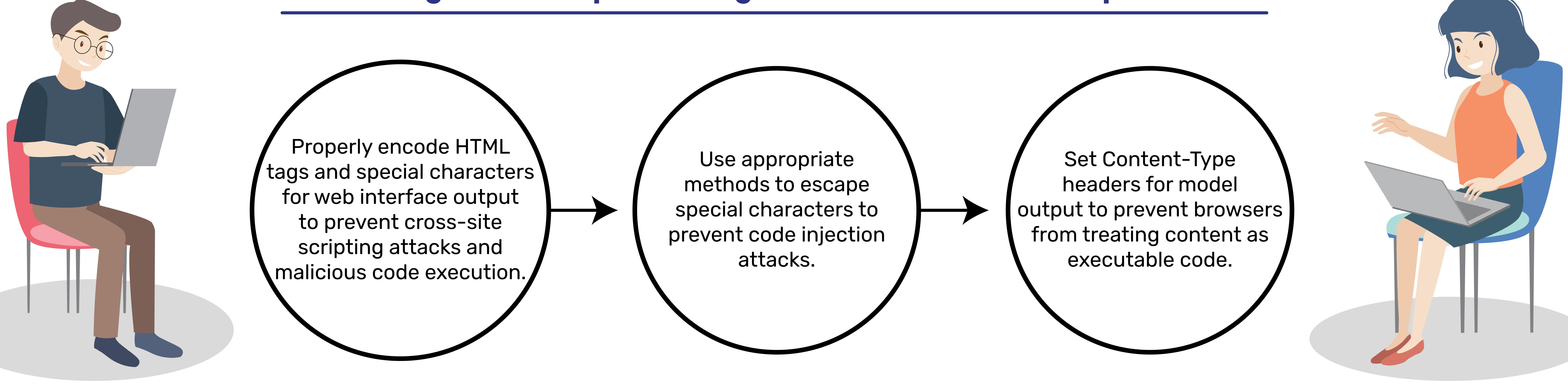


# Solutions to Insecure Output Handling

#### 1. Treating Model Output as Untrusted User Content and Validating Inputs:



#### 2. Encoding Model Output to Mitigate Undesired Code Interpretations:



#### 3. Penetration Testing (Pentesting) for Uncovering Insecure Outputs:

