| **Vulnerability Type** | **Description** | **Where to Add** |
| --- | --- | --- |
| **SQL Injection** | Using string concatenation instead of parameterized queries | In user-service DB calls |
| **Missing Input Validation** | No type/format checks on user inputs | Both services |
| **Hardcoded Secrets** | Hardcoded DB passwords, keys, etc. | In future if we add config files |
| **Outdated Dependencies** | Add a vulnerable package/version in requirements.txt | Both services |
| **Exposed Stack Traces** | Letting Python errors show in the response | Don't use try/except |
| **No Auth** | APIs are public, no auth or rate-limiting | Both services |
| **Insecure Headers** | Not setting security-related headers | Flask default misses this |

⚠️ Vulnerabilities to Simulate