**Security Checklist**

|  |  |  |
| --- | --- | --- |
| **Security item** | **Check Performed** | **Result (Pass/Fail)** |
| Input Validation | User inputs are sanitized (no script injection possible) | Pass |
| |  | | --- | |  |  |  | | --- | | Input Validation | | |  | | --- | | SQL injection attempts are handled safely |  |  | | --- | |  | | Pass |
| Input Validation | Special characters in inputs are accepted or handled without errors | Pass |
| Input Validation | Session tokens are securely generated and stored | Pass |
| Input Validation | Incorrect data types (e.g., numbers where strings expected) handled properly | Pass |
| Input Validation | Command injection attempts are not executed | Pass |
| |  | | --- | |  |  |  | | --- | | Session Handling | | Session expires after set idle timeout (e.g., 10-15 mins) | Fail |
| Input Validation | |  | | --- | |  |  |  | | --- | | Bot prevents directory traversal attempts (../../etc/passwd) | | Pass |
| Bot Misuse | Bot does not repeat sensitive user input back (to prevent phishing replay) | Pass |
| Bot Misuse | Bot responds safely to abnormal or malicious input (no crashes) | Pass |
| Bot Misuse | Bot fallback response is triggered for unsupported or strange queries | Fail |