Security Vulnerabilities & Recommendations

1. Buffer Overflow Risk

- **Issue:** The `buffer` array (`char buffer[1024]`) may overflow if an attacker sends more than 1024 bytes.
- **Fix:** Use `recv()` with a size limit and ensure safe handling.

2. Lack of Input Validation (HTTP Request)

- **Issue:** The server does not check if the received request is well-formed, which can lead to **request smuggling or injection attacks**.
- **Fix:** Implement basic validation before processing requests.

3. Hardcoded HTTP Response

- **Issue:** The server always responds with a static message. Attackers can exploit this to inject malicious content.
- **Fix:** Implement **content security policies** and ensure responses are dynamically generated.

4. No Logging & Monitoring

- **Issue:** No logs are generated, making it hard to track attacks.
- **Fix:** Use **syslog** or a logging framework.

5. No Secure Communication (No TLS/SSL)

- **Issue:** Data is transmitted in **plaintext**, making it vulnerable to **Man-in-the-Middle (MITM) attacks**.
- **Fix:** Use **OpenSSL** or another TLS library.