Security Plan

This security plan outlines key measures to protect the website from common threats while ensuring data integrity and secure access.

---

1. CORS Restrictions (Only Trusted Origins Can Access APIs)

Objective:

Prevent unauthorised domains from making requests to the API.

Implementation:

- Configure CORS (Cross-Origin Resource Sharing) to allow only trusted origins (e.g., https://website.com).
- Block all requests from unknown or unverified domains.

Expected Outcome:

- Prevents unauthorised API access from malicious third-party websites.

---

2. Input Validation (Sanitized User Inputs)

Objective:

Protect against XSS (Cross-Site Scripting), SQL Injection, and other input-based attacks.

Implementation:

- Enforce strict input validation for all user-provided data (e.g., location search).
- Sanitize and escape special characters to prevent injection attacks.

Expected Outcome:

- Prevents malicious input that could lead to data breaches or website defacement.

---

3. HTTPS Enforcement (Secure Data Transmission)

Objective:

Ensure secure communication between users and the server.

Implementation:

- Enforce TLS 1.3 (HTTPS) for all communications.
- Redirect all HTTP requests to HTTPS.

Expected Outcome:

- Prevents Man-in-the-Middle (MITM) attacks.
- Ensures end-to-end encryption of transmitted data.

---

4. Limited HTTP Methods (Only Allow GET Requests)

Objective:

Minimize attack surface by restricting unnecessary HTTP methods.

Implementation:

- Allow only GET requests for public API endpoints.
- Block PUT, POST, DELETE, and other methods unless explicitly required.

Expected Outcome:

- Prevents unauthorized data modification.
- Reduces the risk of API misuse and accidental data overwrites.

Conclusion

By implementing these five security measures, the website will be safeguarded against unauthorized access, data manipulation, and common web vulnerabilities while maintaining seamless functionality for users.