**Web Security Practices:**

1. HTTP Throttling: Limiting the number of requests from a certain IP address for preventing DOS attack
2. Authentication token should be provided via response header
3. Provide proper JSON encode-decode before writing JSON body
4. Avoid sending cookies for maintaining stateless principle and security(if needed, use encryption-decryption policies
5. CSRF(Cross Site Request Forgery) attacks are used to send malicious requests from an authenticated user to a web app, this must be prevented
6. Must provide user agent protection by providing user agent to prevent malicious requests
7. API key must be used for authentication
8. Bearer authentication must be implemented
9. JWT(JSON web token) should be used to transfer JSON data between two parties
10. Project Structure should be maintained appropriately for better security