Project Phase 6: Security Recommendations

a. What is your security recommendation? Why did you choose it?

Use secure random number generation for all random values in the game, especially for user-related data such as high scores or game progress. This ensures that any generated data is unpredictable and secure, which is critical to prevent potential attacks that exploit predictable random values.

b. Who does the recommendation benefit (end-user, developer, etc.)?

This recommendation primarily benefits the end-users by protecting their data and the integrity of the game. It also benefits developers by safeguarding the app against potential security vulnerabilities.

c. If the recommendation was found somewhere other than the provided checklist, include a link to it.

The recommendation is based on the Android App Security Checklist: <https://github.com/muellerberndt/android_app_security_checklist>

d. When would the recommendation have to be implemented (based on how serious the security risk is)?

The recommendation should be implemented during the initial development phase or early in the project lifecycle. The use of secure random numbers is crucial for preventing serious security risks, such as unauthorized access or data manipulation.

e. Why do you think your project needs your recommendation?

This is essential for the project to prevent attacks that could exploit predictable random values, which can compromise user data and game integrity.

f. How do you think your recommendation could be applied? How feasible would the implementation be?

This can be applied by using well-established libraries like 'react-native-crypto' to generate random numbers. The implementation is feasible and straightforward, as it involves replacing any non-secure random number generators with secure alternatives.