Prabhnoor Singh

**What is your security recommendation? Why did you choose it?**

I would recommend using secure communication using HTTPS/TLS to ensure that user data is protected from external malicious actors,

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

It would benefit end users as their data will be safe and won’t be exposed to external unauthorized entities.

Secure communication will be the best option for the developers as it is used in any mobile application that send and receive data.

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

This recommendation is part of the Android App Security Checklist under secure communication.

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

The recommendation should be implemented in the final stages of the coding process and before the testing.

**5. Why do you think your project needs your recommendation?**

When the leaderboard stats are added, data will travel between the app and server and using HTTPS/TLS encryption protects against data breach and data tampering.

**6. How do you think your recommendation could be applied?**

The plan will go as following:

* Communication should use HTTPS endpoints instead of HTTP.
* APIs hosted should be secured with SSL certificate.
* Using libraries like Retrofit (with OkHttp)

**7. How feasible would the implementation be?**

This is highly feasible and straightforward as many hosting services support HTTPS by default. It required low effort to implement and requires minimal changes to configuration.