1. the first easily noticable weakness is MITM,

once the information of the requests has left the client app, there is no way of knowing whether the information got to out destined server or not, the same goes the other way around, we can never be certain whether the information the client receives came directly from the server.

2.code injection is also a discernable weakness,

since the clients input strings of information directly to our console, theoretically it can be manipulated to be treated as code and be used to harm the system.

3. the encryption we used has a very low chance of generating the same key twice, but it is not zero.

its highly unlikely to cause any harm, but the option for it to fail and allow multipule accounts still exists.

4. information leakage is also an expected flaw, since we implemented no counter measures besides the standart verifications that are provided in the librarys we used.