CS673: Security

**OWASP – Top 10 Mobile Risks 2014**

[**https://www.owasp.org/index.php/OWASP\_Mobile\_Security\_Project#tab=Top\_10\_Mobile\_Risks**](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks)

**M1: Weak Server Side Controls**

Our application uses a token in order to access different APIs in our server. Without the token, the requests would not be possible.

**M2: Insecure Data Storage**

We are not storing our data sensitively. Usernames are available as long as we have a token. Password and tokens are stored within the Django server.

**M3: Insufficient Transport Layer Protection**

Our information may be exposed over the network if the user shares same network.

**M4: Unintended Data Leakage**

We have some information stored locally mainly the username and token, so that we don’t have to request for a token everything we send an API request. This is a vulnerability as we can expose our sensitive information like our token.

**M5: Poor Authorization and Authentication**

Our authentication only works if the user is online.

**M6: Broken Cryptography**

We did not look into encryption for our data.

**M7: Client Side Injection**

Multiple requests can cause problems with database.

**M8: Security Decisions Via Untrusted Inputs**

We have not implemented permission levels. As a result, this vulnerability will not apply to our application yet since we did not grant special user access to anyone.

**M9: Improper Session Handling**

We have to make sure our session token isn’t actually shared outside of the application requests.

**M10: Lack of Binary Protections**

We did not incorporate any binary protections.