Owasp or rather Open Web Application Security Project are a set of guidelines that relate to the security in the IT industry. The Owasp project is determined to providing up to date security outlines/concerns. Owasp project main principles are encompassed in a Top 10, the top 10 are as follows Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfigurations, Cross-Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities and Insufficient Logging & Monitoring. These top 10 are what they list as the most important security risks that face development of applications, essentially they list what the vulnerabilities of app development are that can in turn lead to security risks.

In my development I implemented a register and login feature to my app as I security feature and it does match some of the Owasp principles, one being that of Authentication which is based off Broken Authentication from the owasp top 10. But essentially a user needs a password linked to their username that they set when the registered for the app and will not be able to access the app without the correct combination of username and password. Authentication needs to take place between the password tied to the specific username before the user is allowed into the app without the correct authentication the user will not be able to access the app or their account.