CS 594—Enterprise and Cloud Security
Assignment Two—Access Control—Rubric

Demonstrate working app (25 points) (*Video*)

1. ▣ **(10 points)** Adding users
2. ▣ **(10 points)** Posting messages
3. ▣ **(5 points)** Moderating (deleting) messages

Authentication tests (20 points) (*Video*)

4. ▣ **(5 points)** Login failure with invalid password
5. ▣ **(5 points)** Login failure with invalid TOTP code
6. ▣ **(5 points)** Login failure with invalid role
7. ▣ **(5 points)** User name is displayed when successfully logged in

Authorization tests (15 points) (*Video*)

8. ▣ **(5 points)** Admin user cannot access poster or moderator paths
9. ▣ **(5 points)** Poster cannot access admin or moderator paths
10. ▣ **(5 points)** Moderator cannot access admin or poster paths

Securing the app (15 points)

11. ▣ **(5 points)** In `ChatWebApp`, use annotations on `AppConfig` class to specify custom forms-based authentication with a relational database to store user information. Configure password hashing in authentication to be consistent with that used by the service when adding or updating user information.
12. ▣ **(5 points)** In `ChatWebApp/WebContent/WEB_INF/web.xml`, define path-based, role-based access control.
13. ▣ **(5 points)** Require SSL with user data constraint (see `web.xml`).

Securing the service (20 points):

14. ▣ **(10 points)** All operations in MessageService have appropriate RBAC specifications (use `@RolesAllowed`).
15. ▣ **(5 points)** `@RunAs` used to allow `ChatInit` to run with role “admin” to access the service.
16. ▣ **(5 points)** `MessageService` addMessage: Make sure that the poster is posting a message under their own username (check the username in the message against the logged-in user).

Completed rubric ▣ **(5 points)**

Total: 100