

## Report 5

Gosling

Zhunussova Meruyert - 200103534

Bekmagambetova Diana - 200103329

**Diana** is responsible for:

- Running HTTPS server, for starting to use HTTPS server, I generated a TLS certificate. So, used the crypto/tls package in the standard library, which includes a generate\_cert.go tool. This tool can be used to easily create a self-signed certificate.
- Implemented basic signup and login functionality for users. These techniques can be useful for securing web applications and providing secure access to users. A users can register by visiting a form at /user/signup and entering their name, email address and password. Information will be stored in a new users database table. Then user will redirected to /user/login and entering their email address and password.
- Also was added database checking to see if the credentials user entered match one of the users in the users table.

**Meruyert** is responsible for:

Having the ability to log users in and out of our GOsling website is not enough, that's why we need to do something useful with that information and added some authorization checks.

- User authorization

1. Only authenticated users can create a new request
2. Navigation bar changes depending on whether a user is authenticated or not.

Authenticated users should see links to Home, Create snippet and Logout. Unauthenticated users should see links to Home, Signup and Login.

- CSRF token

To protect our website from CSRF attacks.

1. If user logs into our website. Our session cookie is set to persist for 12 hours, so they will remain logged in even if they navigate away from the website.
2. Since the user is still logged in to our website, the request is processed with their privileges. Completely unknown to them, a new request will be added to our database.