Week 2: Implementing Security Measures

1. **Implementing anti-CSRF packages such as the OWASP CSRFGuard**

I implemented an anti-csrf packages to prevent csrf or xsrf attacks, I implemented

Csrf tokens for all views of the website so the user's data is safe even when they are logged in or the website session is still active. The cookie parser is used to keep them out of third-part sites.

Credential are sent securely through HTTPS and handled by an authentication mechanism (e.g:bcrypt,session)

I added csrf token to both logins and registrations of user and admin when the email and password are accessed by the user or admin.

2. **Content Security Policy (CSP) Header Not Set**

Handling input validity and securing passwords by making a policy for password s to be 8 characters long. This policy applies when the new user is registering their new account on the website.

3. **Missing Anti-clickjacking Header**

Added X-frame options to prevent iframe tags to be executed tin the code which can lead to a fake website opening up appearing as a legitimate website.
Reduced the background opacity so any other, malicious website is not running in the background and stealing the user credentials from any search options or user input fields like for example bank accounts.