Agenda:

- MVP feedback
  - Routes suggestions
- Demo work since MVP
- What should we use for verification of employers?
  - Admin account
  - Secret password
  - API Token via email with button
    - Send a link with a post request link that allows admins to verify the account with a validation token (given to admins only)
  - (If either 2 or 3, why, and what is the difference? What are the pros and cons of each)
- Does using templates (ex: req.body) convert to strings/sanitize all input and can we prevent cross site scripting and script injection
- CSRF: how to pass and receive form tokens (does handlebars interfere)
- Can we just assume server is in EST?
- Future plans
  - Discuss our future plans: UI work and Security is all that we think are left
  - Advice on what we should do going forward

Progress Report:

- Progress
  - Deadlines for job postings
  - Deleting job postings
  - Rejecting, starring, unstarring, deleting, withdrawing, saving custom applications
  - Filtering and sorting
  - Additional types of questions
  - Limit number of applications
  - Mitigating brute force login
  - Hashing passwords
  - UI update
  - Some security
    - Hashing passwords
    - Brute force
- Milestones Achieved:
  - Pretty much added all new features for Student and Employer usages
  - Was able to update UI (almost to final version)
- Milestones Missed:
  - Security stuff with tokens
- Difficulties Encountered:
  - Figuring out security/CSRF
- Changes
  - No significant design changes, but changes in ideas for security

        - Employer verification:
        - Considering not handling network eavesdropping

Meeting Minutes:

- MVP
    - Most/all of features are there, so it seems to work fine
        - Back button bug
    - In code, in model for Common.js, there is question defined but it was defined in two places (with one as a global)
        - Solved
    - Remove all unused code
    - Application/customid/star rather than a separate route for star/unstarred
        - Have “status” in the body
    - Full app in routes seems odd
        - Not sure what to make of it
- Demo work since MVP
- Verifying token
    - OK if use secret password or API (although not common practice, but acceptable)
- CSRF
    - OK to use separate form tokens but also OK to generate one csrf token that is used for all forms
- OK to assume servers are in EST
- Demo:
    - Demo the full app this Thursday