Since our app is focused on allowing students access to their university data, there is much sensitive data that we will need to protect against attacks and exposure. The most sensitive pieces of data will be student ID’s, usernames, passwords, schedules, permissions, and more.

As Chris’s mentioned, we can protect our HTTPS requests by using SSL and TLS to encrypt our requests as they are sent over the network. For example, when users are logged in and making changes to their schedule, we will need to make sure our GET/POST/PUT/DELETE methods are encrypted before they are sent from the client to the server. We can even get a free certificate from a site like letsencrypt.com or startSSL. A good tool for keeping our HTTP headers secure would be something like helmet that works with Node.

Also, we can secure session cookies by restricting the client to access the cookies with a script, preventing attacks that attempt to access cookie contents. This can be done by using the httpOnly flag in express.

Lastly, we will want to prevent user input from being vulnerable to XXS or SQL injection, and this will mostly be done by using button selections to perform actions. However when text is used as input, we can use a tool like express-validator in conjunction with body-parser that makes use of regular expressions and escape characters to validate input formats like email and dates.