Project Schedule Through 8/17

8/9

1. Evan- Maintain State in Transactions, Set and Read Cookies
   1. Login to be able to put their favorite music into a users table and to change the contents of the table, but the whole table is displayed with username: music tastes
   2. If a cookie is set (isset($\_COOKIE[‘name’])) then they can change their entry in the table/add a new entry but delete the previous maybe 🡪 login.php
2. Nick- Fill in the database tables

8/10

1. Evan- PHP script to process form data (Texas Music Form)
2. Nick- Validate HTML and CSS written so far (home page, latin music page, bibliography, about us, contact us, fill in database tables)

8/11

1. Evan- Texas Music Map- Figure out how to code clicking a part of the picture will open a new page with the information from that city
   1. Click on a city on the map, it takes you to another page and tells you Popular musicians from there, what genres were popular, what popular songs came out by Texas musicians, and a major event that impacted music in Texas at that time
2. Nick- Popular Texas Music Page
   1. For each decade, describe what Texas music was like then have the user add their name to a list of Texas favorites

8/12

1. Evan- DHTML Feature
   1. [Dynamic HTML (utexas.edu)](https://www.cs.utexas.edu/users/mitra/csSummer2021/cs329/lectures/dhtml.html)
   2. Javascript application where you getElementById and add your name and your favorite Texas song, artist, or genre to a growing list after reading about the music in Texas from different decades
2. Nick- Application of AJAX 🡪 brainstorm or code if you get an idea

8/13

1. Evan and Nick- Texas music map and filling in database tables

8/14

1. Evan and Nick- You must include the following security features in your web application:
   1. Store passwords in encrypted form. Incorporate the SHA-256 Cryptographic Algorithm in JavaScript on the client side. Use the crypt() function in PHP.
   2. Impose size restrictions on all input data. Run a filter function that will purge all unacceptable characters from the input.
   3. Use mysqli\_real\_escape\_string() judiciously to prevent SQL injection.
   4. Take steps to prevent Cross Site Scripting using strip\_tags() and htmlentities().

8/15

1. Study for Test 3

8/16

1. Evan and Nick- Finish all applications and pages (make sure everything works)

8/17

1. Evan and Nick- Make website look professional and turn it in