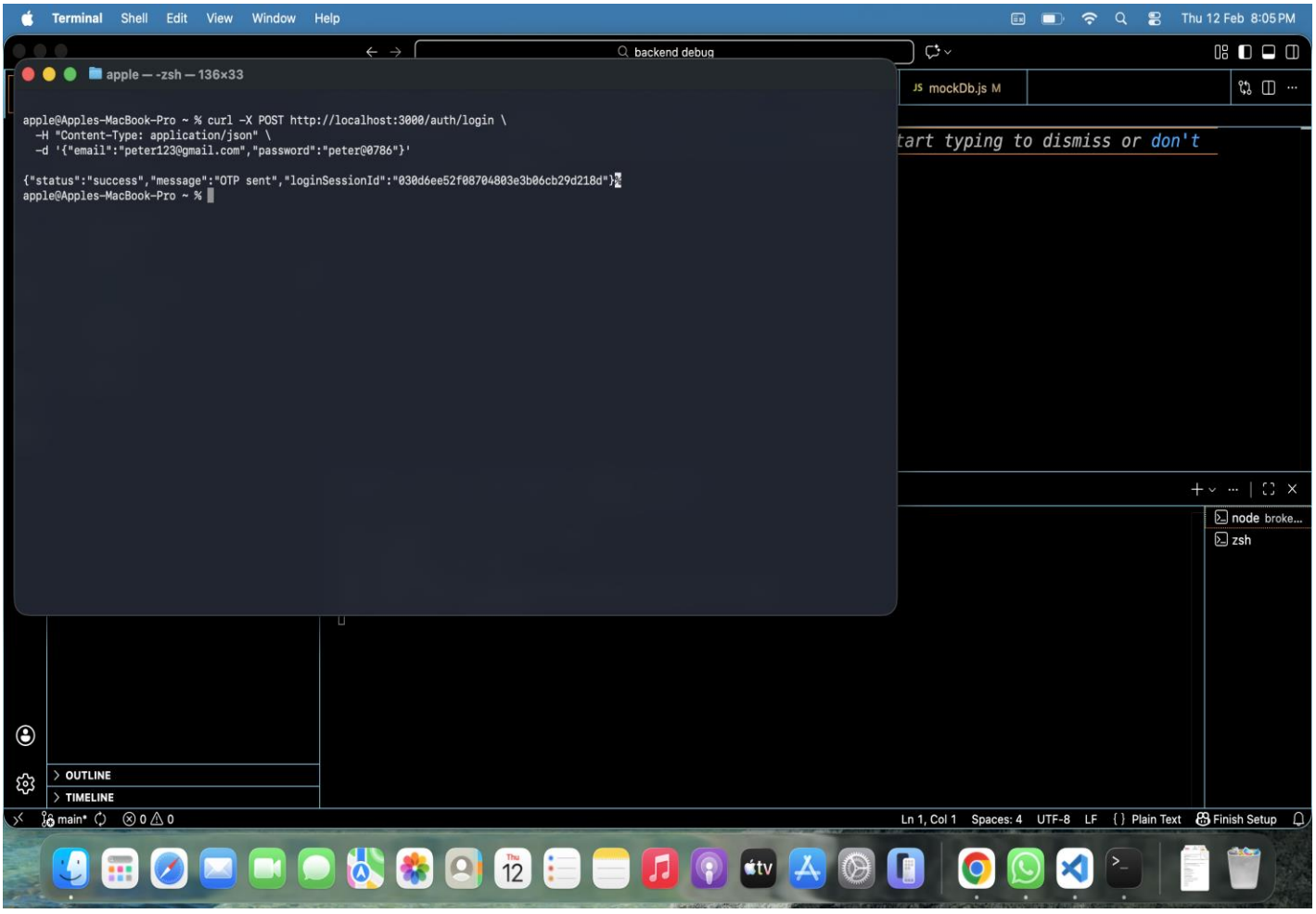
Task 1: Fix Login

Endpoint: POST /auth/login The server should generate a session and log an OTP to the console.

Test Command:

```
curl -X POST http://localhost:3000/auth/login \
 -H "Content-Type: application/json" \
 -d '{"email":"<YOUR_EMAIL@example.com>","password":"password123"}'
```

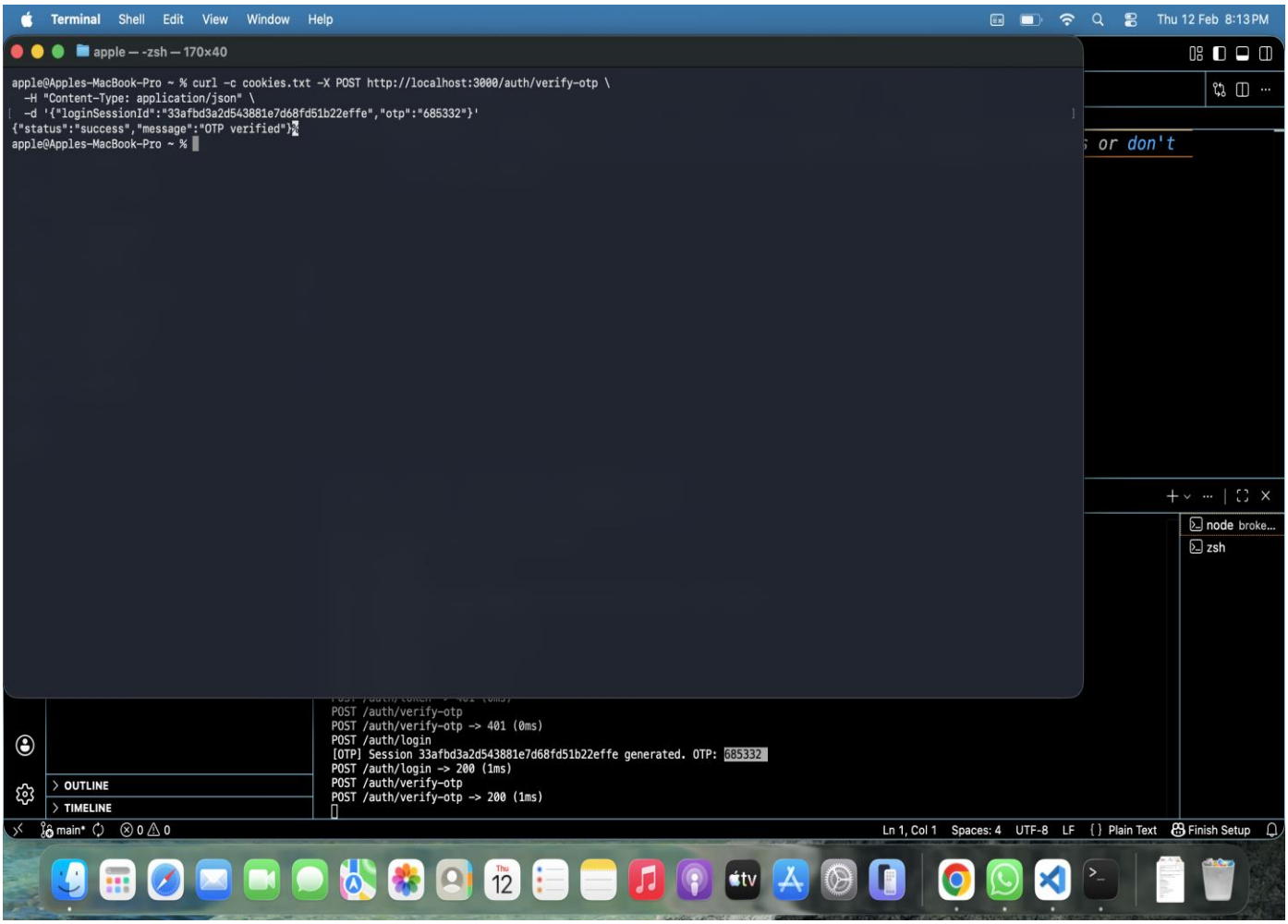


Task 2: Fix OTP Verification

Endpoint: POST /auth/verify-otp The server fails to verify the OTP correctly. You need to find out why. *Hint: Check data types and how cookies are set.*

Test Command: (Replace <loginSessionId> and <otp> with values from Task 1)

```
curl -c cookies.txt -X POST http://localhost:3000/auth/verify-otp \
  -H "Content-Type: application/json" \
  -d '{"loginSessionId":"<loginSessionId>","otp":"<otp_from_logs>"}'
```

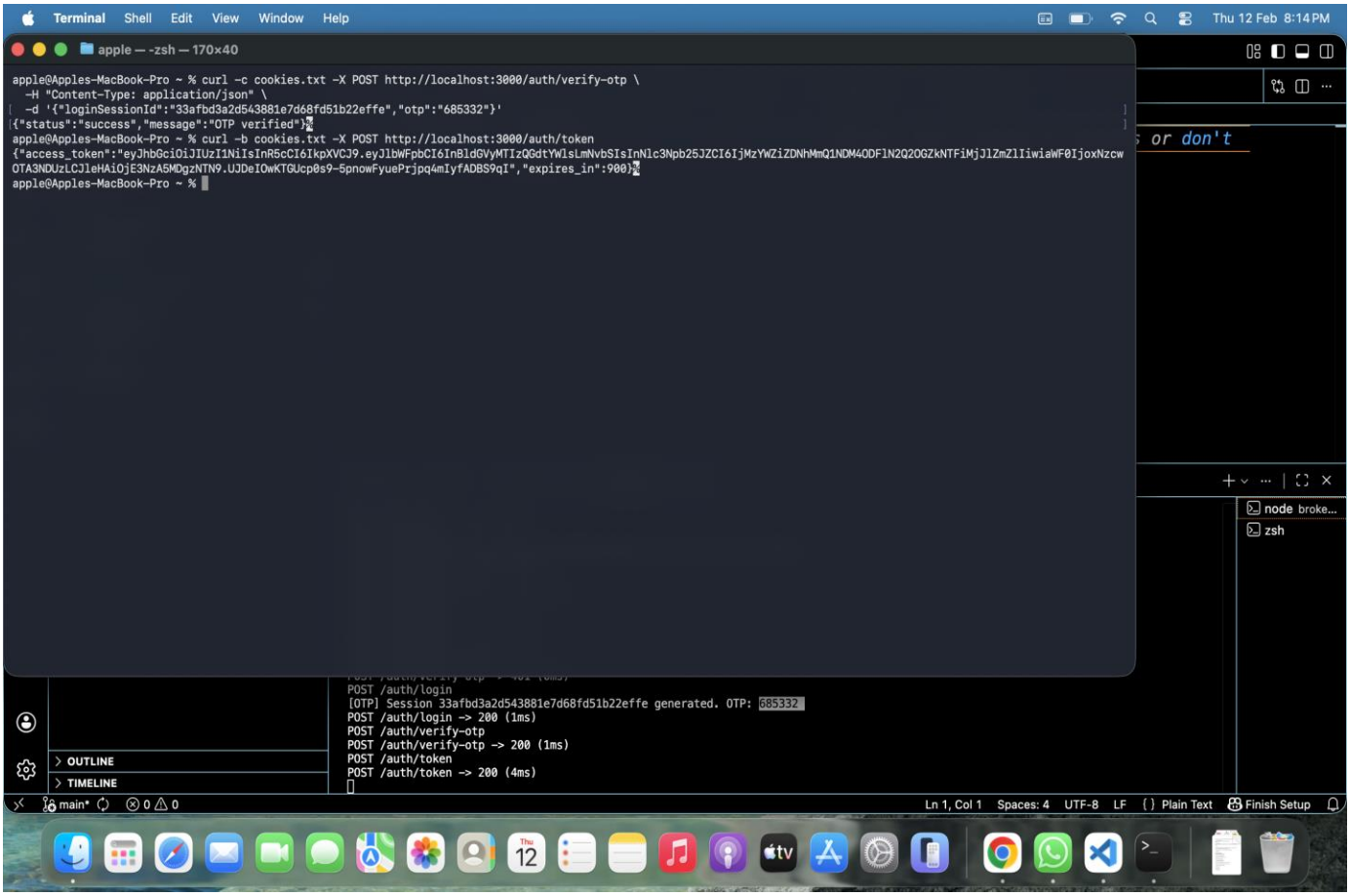


Task 3: Fix Token Generation

Endpoint: POST /auth/token This endpoint is supposed to issue a JWT, but it has a bug in how it reads the session.

Test Command:

```
# Uses the cookie captured in Task 2
curl -b cookies.txt -X POST http://localhost:3000/auth/token
```



Task 4: Fix Protected Route Access

Endpoint: GET /protected Ensure the middleware correctly validates the token.

Test Command:

```
# Replace <jwt> with the token from Task 3
curl -H "Authorization: Bearer <jwt>" http://localhost:3000/protected
```