Lesson 8

Authentication

- Should anyone be allowed to write a review?
  - Yes

- Should anyone be allowed to change Olive Garden’s menu or location?
  - No

We need authentication!

Authentication

Two popular methods

- Session based
- Token based

Session Based

- Server creates a “session” object when a client logs in
- It responds to the client with a sessionID
- The client stores this ID in a cookie and then sends it in every subsequent request
- The server reads the ID and verifies that it’s a valid session ID
- When a client “logs out”, it clears the cookie and tells the server to delete the “session” object
- Kind of complicated, we won’t do it

Token Based

- When a user logs in, the server responds with a “token”
- A token is an object with information about the client, and it is a key that represents what you’re allowed to access
- The server stores nothing
- Every time a client makes a request, it includes the token
- The server decodes it and sees who the client is. Using that it either allows the request or denies it
- The token automatically expires after some time

Token Based - OAuth

- Sometimes, you see “Log in with Google” or “Log in with Facebook”
- Client logs in to Google and gets an OAuth token from Google
- It sends the OAuth token to our server
- The server asks Google for information about this OAuth token
- Once it verifies it, the server creates its own token (like the previous slide) and responds with this to the client
- Client then uses this token as usual, sending it on every request (like previous slide)

Even simpler: Basic Auth

- Instead of fancy tokens, just send the actual username and password every request
- Server can easily verify a username and password

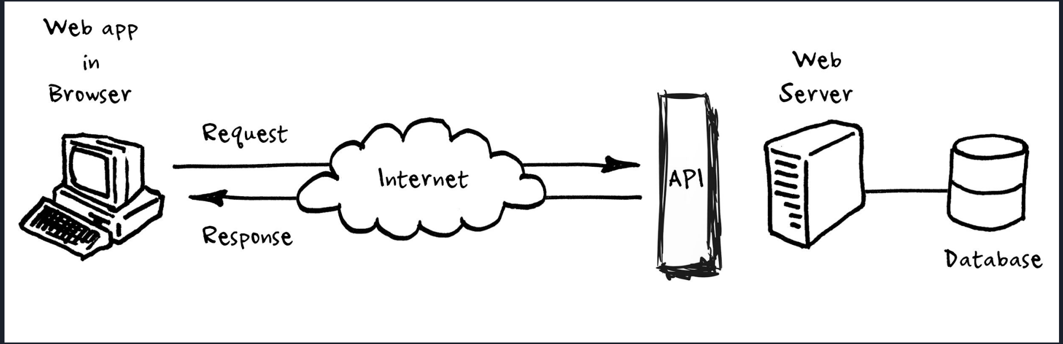
Verification

- How do we store passwords?

- Hashing
    - Store hashed password in database when user creates account
    - When user logs in, hash the password they typed in
    - Compare hashed password in database to hashed password they typed in

What’s an API?

- Application Programming Interface
- Allow applications to communicate w/ each other
- Can get data from other sources
- HTTP requests don’t need a front end
  - Data returned w/ JSON



API Example

- We wanna get all the tweets that used #TGIF
- Time - consuming to ask Twitter to send a spreadsheet
  - Data would also become outdated
- We need a way to get LIVE data → API
- Twitter API could return live data when called

Using an External API

- ACCESS API → API RETURNS JSON → PARSE JSON → USE DATA
- Zomato API
    - Search location
    - Get location id
    - Search restaurants by location id
    - Return list of restaurants

LIVE CODING SESSION