Rest APIs and Secrets

Design and Development, Software Engineering

Admin

- Which one are we supposed to talk about today?
  - Read chapter 1 in pragmatic programmer
  - Listen to “The Programming Podcast” podcast (linked on the class web site) episode from Dec 4, 2025 (three links below)
    - https://www.youtube.com/watch?v=ap9kVWOs-fk
    - https://podcasts.apple.com/us/podcast/the-job-search-crisis-why-3-3-million-people-are/id1778885184?i=1000739722249
    - https://open.spotify.com/episode/5JxdklEjKVqbi1aFsmlH18
  -

JSON

- How Many of you have done work with APIs and JSON?

JSON

- How Many of you have done work with APIs and JSON?
- Depending on the answer we might be skipping some slides

Code Examples

- The code examples in the following slides are in java because python is too easy
  - import requests
  - response = requests.get(<your location here>)
  - Response = requests.post()

Data on the Internet

- Once upon a time
  - Data on the web (http/https) was all web pages intended to be viewed by people.
    - If we wanted to have a program read the data – need to ‘scrape’ the page.
- Back in 2000, Roy Fielding proposes REST framework (Ph.D thesis)
  - REpresentational State Transfer
  - Provide a way for web server to give data directly to program clients.
  - In last 5-10 years really used a lot

json

- json: JavaScript Object Notation
  - pronunciation note
  - json notation used by many RESTful interfaces to provide data
  - Says javascript but not really
  - Java vs javascript?
  - Java is to javascript as?

json

- json: JavaScript Object Notation
  - pronunciation note
  - json notation used by many RESTful interfaces to provide data
  - Says javascript but not really
  - Java vs javascript?
  - Java is to javascript as?
    - Car is to Carpet
- Official json spec
  - http://www.json.org/

Sample json

From https://openlibrary.org/dev/docs/api/lists


```
{
  "links": {
    "self": "/people/george08/lists.json",
    "next": "/people/george08/lists.json?limit=5&offset=5"
  },
  "size": 12,
  "entries": [
    {
      "url": "/people/george08/lists/OL13L",
      "full_url": "/people/george08/lists/OL13L/Various_Seeds_for_Testing",
      "name": "Various Seeds for Testing",
      "last_update": "2010-12-21T00:46:17.712513",
      "seed_count": 13,
      "edition_count": 13181
    },
    {
      "url": "/people/george08/lists/OL97L",
      "full_url": "/people/george08/lists/OL97L/Time_Travel",
      "name": "Time Travel",
      "last_update": "2010-12-17T18:27:14.781336",
      "seed_count": 5,
      "edition_count": 838
    },
    ...
  ]}
```

From the web

- To get data from the web we use what protocol?

From the web

- To get data from the web we use what protocol?
  - http
  - Or https
- Java 11-17 (and of course java21) improved java's support for getting data from http sources quite a bit
- Added

```
java.net.http.HttpClient;
java.net.http.HttpRequest;
java.net.http.HttpResponse;
```

HttpClient

- The HttpClient class manages the connection from your program to the website
- Like so much of the java standard library
  - Uses factory functions.
  - Constructor is protected to keep you from directly using it.

```
var dataGrabber = HttpClient.newHttpClient();
```

  - Use send(<params here>) function on dataGrabber to actually get data
  - But we need more before we have the right params

HttpRequest

- The HttpRequest object packages up everything we need to do to make a request of a website
  - Allows for significant customization for advanced applications
  - But perfectly usable for early learners like us as well.
  - Lots of tutorials do this in one step – lets learn it in two.

```
var requestBuilder = HttpRequest.newBuilder();
var dataRequest = requestBuilder.uri(

URI.create("http://universities.hipolabs.com/search?name=Young")).build();
```

  - Once again use a factory to build the object.
  - Then we add the web location and call build.

Making the request.

- Now we have everything ready to ask the server for data
  - But as soon as we touch the network what do we have to think about?

Making the request.

- Now we have everything ready to ask the server for data
  - But as soon as we touch the network what do we have to think about?
  - EXCEPTIONS!?!?!
    - It could be as simple as the wifi being off on your laptop
      - Or the server is down
      - Or the server was up, but network cable gets cut
      - Or more…….

Making the request.

- Now we have everything ready to ask the server for data

```
HttpResponse<String> response = null;
try {
    response = dataGrabber.send(dataRequest, HttpResponse.BodyHandlers.ofString());
}catch(IOException e){
    System.out.println("Error connecting to network or site");
}
catch (InterruptedException e){
    System.out.println("Connection to site broken");
}
```

  - Two types of exceptions possible
  - Hi-lighted text says treat the main bit of data returned as a string.

What if it went wrong

- If the connection failed
  - In a bigger program we might try to recover
  - For this simple example just fail and exit

```
if (response == null ){
    System.out.println("Something went terribly wrong, ending program");
    System.exit(-1);
}
```

And in python

- Lets take a super quick look at how we would get that university data in python.

Http Protocol

- So far we are just doing Http get
  - What else is available?

Http Protocol

- So far we are just doing Http get
  - What else is available?
    - POST – very common – especially for forms
      - Which our program sometimes use
    - DELETE
      - Less common, but sometimes used.
    - PUT
      - Even less common
    - PATCH
      - I’ve not seen this used, but I’m not a webdev

Two step login→get data

- Of course if you have multiple end points what is the issue with getting data?
  - With login on one endpoint and then data download (requiring login) on another

Two step login→get data

- Of course if you have multiple end points what is the issue with getting data?
  - With login on one endpoint and then data download (requiring login) on another
  - Web is ‘stateless’
  - So either have to use session, or send bearer token

Session Example

```
import requests
import json

session = requests.Session()
session.post(url="http://localhost:8000/api/v1/member/login/",
                    json={"email":"redacted","password":"redacted"})
value = session.get("http://localhost:8000/api/v1/meeting-rooms/available/")
print(value.text)
```

Bearer Token Example

If you have a django server, the login returns a json/dictionary with two keys

You need the ‘access’ value to pass to other endpoints to show authentication.

```
result = requests.post(url="http://localhost:8000/api/v1/member/login/",
                       json={"email":username,"password":password})
if result.status_code == 200:
    response = json.loads(result.content)
    token = response["token"]

response = requests.get(url="http://localhost:8000/api/v1/meeting-rooms/available/",
                  headers={"Authorization":f"Bearer {token.get('access')}"})
```

Java

- For java use the modern
  - `HttpRequest`
  - `HttpRequest.newBuilder()`
  - `HttpResponse<String>`

To accomplish the same thing.

Retrospective

- Here we are first class after Sprint 1
  - Time for an agile retrospective
  - Anyone done one before?
  - What is it?

Retrospective

- Here we are first class after Sprint 1
  - Time for an agile retrospective!
  - Get in groups (those that didn't sign up last time have been assigned via python's random.choice
  - Questions to answer:
    - What went well
    - What didn't go well
    - What do we wish we knew (more academic than industry)
    - What will we do differently next time
  - Then we will have a report out from the groups

Secrets

- In these slides we were using an API that doesn’t require an API key
- But today most require a key
  - Or oAuth
- And of course we put all that code up on github
  - So what could possibly go wrong?
-

Secrets

- In these slides we were using an API that doesn’t require an API key
- But today most require a key
  - Or oAuth
- And of course we put all that code up on github
  - So what could possibly go wrong?
- So yeah – we don’t want that API key out on the web where people can use it

It’s on my door

Secrets

- One common solution is to use a ‘Secrets’ file,
  - maybe api_secrets.py
  - That file is used locally, but not put up on github
  - Make sure to add it (api_secrets.py) to “gitignore” so that it doesn’t get added and pushed accidentally
    - Lets try something simple
    - https://serpapi.com/playground

Lets look at serpapi site – they give you code in many languages for getting their data. **BUT**, they embed the secrets into the code. You would never want to put those API keys into github that way.

- Lets use python to make it easy to start with.

Secrets.py

- Introduce api_secrets.py.
  - Or apiSecrets.go
  - Or apiSecrets.java
- Put it in gitignore
- Was a popular approach a few years ago – why less so now?
-

Secrets.py

- Introduce api_secrets.py.
  - Or apiSecrets.go
  - Or apiSecrets.java
- Put it in gitignore
- Was a popular approach a few years ago – why less so now?
  - What was the Tea App in summer 2025?
  - What went wrong?

dot-env

- Another approach
  - Use a hidden file of environment variables in key-value pairs
  - dot-env library came out of ruby community
  - Versions ported to more widely used languages like python, java etc
  - Docs for python version
    - https://pypi.org/project/python-dotenv/#getting-started
  - Java https://github.com/cdimascio/dotenv-java
  - Go https://github.com/joho/godotenv

- Two common use cases (from docs)
  - Load from .env file to os.environ
  - `from dotenv import load_dotenv`
  - `load_dotenv()  # reads variables from a .env file and sets them in os.environ`
  - Load from .env file to python dictionary
  - `from dotenv import dotenv_values`
  - `config = dotenv_values(".env")  # config = {"USER": "foo", "EMAIL": "foo@example.org"}`
  - Either way, secrets now in program
  - But what is the issue?

- Two common use cases (from docs)
  - Load from .env file to os.environ
  - `from dotenv import load_dotenv`
  - `load_dotenv()  # reads variables from a .env file and sets them in os.environ`
  - Load from .env file to python dictionary
  - `from dotenv import dotenv_values`
  - `config = dotenv_values(".env")  # config = {"USER": "foo", "EMAIL": "foo@example.org"}`
  - Either ways, secrets now in program
  - But what is the issue?
    - Attacker that knows how to look for .env can still find secrets.
    - What is the fix?

- Two common use cases (from docs)
  -
  - But what is the issue?
    - Attacker that knows how to look for .env can still find secrets.
    - What is the fix?
    - Store encrypted secrets?
    - Don’t store .env on github surely

Testing on github

- Lets use secrets on github
  - We will use the github secrets mechanism to create a file in the ephemeral docker container during testing that will disappear after the github actions are done
    - The container along with everything ever on it is gone
  - "To create secrets for a user account repository, you must be the repository owner. To create secrets for an organization repository, you must have admin access."

Adding a secret to github

- To add a secret to github
  - On GitHub.com, navigate to the main page of the repository.
  - Under your repository name, click Settings.
  - In the left hand side menu in the security section open the secrets and variables menu
  - Then pick actions
  - The secrets tab is active by default, in the upper right is a green button called "new repository secret" push it
  - Name your secret (name requirements next slide)
  - Put your secret (no quotes!) in the secret text box

Github’s rules for naming secrets

- Secret name rules
  - Names can only contain alphanumeric characters ([a-z], [A-Z], [0-9]) or underscores (_). Spaces are not allowed.
  - Names must not start with the GITHUB_ prefix.
  - Names must not start with a number.
  - Names are not case-sensitive.
  - Names must be unique at the level they are created at.

Building the secrets file

- My file called api_secrets.py is in my gitignore,
  - so I want to rebuild it in the ephemeral docker container in github actions (do .env files similarly)
  - I called my secret LLM_API_KEY, and in my github actions I put the following between Install dependencies and linting
    - My api_secrets.py needs a line like
      - gemini_api_key='<my key here>'

```
- name: Build Secrets
  env:
    API_KEY: ${{ secrets.LLM_API_KEY }}
  run: |
    echo 'gemini_api_key = "'$API_KEY'"' >> api_secrets.py
```

Let’s look at the project

- Let’s look at project 1 sprint 2
  - If we haven’t done so already

If we are one week from first day

- The rest of this is the review of pragmatic programmer

Pragmatic Programmer

- Lets talk about the first chapter of the pragmatic programmer
  - Agency: lots of you will be highly paid professionals in less than a year
    - You'll be in a position to do great things and responsible when things go terribly wrong (just ask Knight Capital)
    - Many of you have not had the chance to take this kind of responsibility
    - But now….

Impostor Syndrome

- There is a lot of discussion these days in the industry about “Impostor Syndrome”
  - What is it?

Impostor Syndrome

- There is a lot of discussion these days in the industry about “Impostor Syndrome”
  - What is it?
  - The notion that many developers have that they don’t know as much as people think they do
  - That they will soon be “found out”
- Opposite and just as bad as “know it alls”
- discuss

Good?

- What is the single best indicator of how good a student is likely to be in this course?

Good?

- What is the single best indicator of how good a student is likely to be in this course?
  - Practice.
    - How much time has the student devoted to the projects in previous classes?
    - Did the student do an internship?
    - Has the student worked on personal projects outside of class
      - Unless the student lets their personal projects get in the way of class projects in which case this becomes and counter indicator
    - Does the student need to work in a way that limits their practice time
  - All boils down to practice.

Practice

- Much of this practice time will be evened out by this time next year.
  - You will spend 100% of your work time on actually doing development.
  - So you will practice your craft more in the first year of work than in 4 years here
  - Prediction: Many ‘aha moments’

Keeping up to date

- Keep Learning
  - My mechanic example
  - ‘Lifetime Learning’ – so important today required by both ABET and New England Commission of Higher Education
  - What did you think of Andy and Dave’s take on lifetime learning?

Keeping up to date

- Keep Learning
  - My mechanic example
  - ‘Lifetime Learning’ – so important today required by both ABET and New England Commission of Higher Education
  - What did you think of Andy and Dave’s take on lifetime learning?
    - A deep technical book a month?
      - Might be a bit ambitious
    - Deep technical books at all?
      - I think so, I’ve done video courses and they are more like web tutorials – great but not as in depth.
    - “Long form” vs “short form”

Pragmatic Programmer

- Language Learning
  - Lets talk about language learning
  - One common criticism of academic programs
    - They teach one language
    - And use it for all classes
      - students come out with blinders on
  - But it is important to learn a couple of languages well
    - (jsantore's opinion) Start with two
      - One compiled language (eg Java, C++, Rust, Go, Kotlin, Swift)
      - One interpreted language (eg Python, Javascript, ruby, php)
  - Then when you know a couple well, then try 'cool kid' languages (eg Erlang, Haskell Clojure etc)

Pragmatic Programmer

- Anything else on chapter 1?

Assignment: If not assigned already, do Assignment 1 sprint 1