**Sprint 3 Week 1**

**Architecture**

Our project can be split into:

* Data collection (web scraping, APIs)
* Data storage (in the Excel file)
* Data analysis (regression models, profit calculations)

Based on this splitting, the most useful architecture would be **Component-based Architecture**

* Individual systems (components) that interact with each other but run separately
* Allows you to easily improve the systems individually and run them together, too
* In our project, our 3 three distinct components all serve different purposes
  + Data collection component - Collecting data from our sources
    - We can collect multiple sources or find most accurate ones
  + Data storage component - Holding our data in a spreadsheet
    - We can query the data to easily access certain information
  + Data analysis component - Calculates the maximum profit
    - We can use this to run regression models and calculations
* These components are combined into a dataflow: Collection → Storage → Analysis

Fatima + Sha

**Security**

* Authentication and Authorization
  + Ensures safety by having people log in before accessing the system
  + Two-factor authentication nearly guarantees that it’s *you* logging in
  + We will use two-factor authentication to ensure that no hacker can get in
  + For the logged in users, we will make sure that they’re authorized by giving them permissions and frequently checking those to make sure they’re up to date
* Logging and Monitoring
  + Tracking all actions made to the system (by web scrapers, APIs, users, etc)
  + See who is contributing to the system (get usage statistics to improve it)
  + If an error occurs, the information can be found (tied to a user, timestamp, etc)
  + This will help us debug errors faster and eliminate security threats faster

**Training**

Our training plan will be divided into two parts.

Initial Training

* Instructional Videos
  + Videos on phishing, using each part of the system, security, and general rules

Continuous Training

* Online Documentation
  + Easily accessible website to see all of the training info and how to use each part of the system (text-based and video-based tutorials).
* Email Checks
  + We will send emails that may be phishing. Users must identify the phishing emails in order to pass the training.
* Security Audits
  + Each period, we will look at the logs and security details to assess the effectiveness of the security system and improve it to match the latest tech.
  + We will update the documentation and also review it with every member.