Christopher Hernandez
Week 12 Research

1. Why would you want to avoid putting credentials in plaintext in your code?
    - It is important to avoid putting credentials in plaintext in your code for security reasons. Placing credentials directly in the code makes them easily accessible to anyone who has access to the codebase. If the code is stored in a version control system or shared with others, it becomes a significant security risk. Malicious actors or unauthorized individuals can easily obtain the credentials and gain unauthorized access to sensitive systems or data. Therefore, storing credentials in plaintext in code is highly discouraged to protect the security and integrity of the systems and data.

2. What is one method that can be used to avoid putting plaintext database usernames and passwords into your code?
    - One method to avoid putting plaintext database usernames and passwords into your code is to use environment variables. Instead of hardcoding the credentials in the code, you can configure the application or the runtime environment to read the credentials from environment variables. Environment variables are variables that are set in the operating system or runtime environment and can be accessed by the application during runtime. By storing the credentials as environment variables, you can keep them separate from the codebase and ensure that they are not exposed to potential security risks. This approach allows for greater flexibility, as the credentials can be easily updated or changed without modifying the code itself. Additionally, it enables better security practices, such as restricting access to environment variables to authorized individuals or using tools to encrypt or secure the environment variables.

Citation: https://towardsdatascience.com/keep-your-code-secure-by-using-environment-variables-and-env-files-4688a70ea286