MSDS 5153 Worksheet—Week 3

Which of the following are common built-in text editors in Linux? (check all that apply)
□ Atom
☒ Nano
□ Sublime
□ DataGrip
☒ VIM
https://support.apple.com/guide/terminal/use-command-line-text-editors-apdb02f1133-25af-4c65-8976-159609f99817/mac

What is the linux command to create a file?
□ open
☒ touch
□ create
□ source

If you made changes to your bash profile, such as adding an environmental variable, how would you ensure those changes went into effect?
□ Re-start your computer
□ Close all terminals then open a new one (Windows)
☒ source ~/.bash_profile (MacOS)
□ Nothing, changes are automatic
https://www3.ntu.edu.sg/home/ehchua/programming/howto/Environment_Variables.html

You should *never* hard-code passwords or secret keys in code.
☒ True
□ False

What is the command to exit vim?
□ exit()
□ quit
☒ :q
□ close

Name and briefly describe 3 ways to manage your credentials.

1. Environmental Variables – These variables follow the KEY = value format and can be stored so that they are available in any new session (using *bashrc*) or just this exact instance (using export shell variable). Once you have saved your environmental variables, you can access them in a jupyter notebook by referencing the KEY. You will be able to upload/share your notebook without your credentials being compromised.
2. .config file – Instead of storing your credentials in variables, you can store them in a text file along with further parameters and initial settings. This file can then be called and parsed using *configparser* to retrieve your credentials. Again, this will eliminate any important information being compromised when sharing your code on other platforms.
3. Via an Application – Many cloud based services have provided a solution to this for users via their own application. For instance, Amazon offers AWS Secrets Manager, Azure offers Key Vault, and Active Directory offers Domain Services (AD DS). These store your credentials in the cloud, allowing you to retrieve and update your passwords seamlessly, and maintaining security for your important information. This option is good for large companies that have many credentials to manage and periodically update.