Week 1 Quiz 2

1. Which practices can help improve your confidence in requesting support in security testing from an LLM?

    - Use newer or obscure libraries to increase the odds those libraries don't have any exploits.
    - Identify whether your LLM has access to information on the web

      Some LLM models can search the web for you to supplement their training data, hopefully providing more up-to-date information about potential cybersecurity threats.

    - Hide the context of your project from an LLM to prevent any potential security breaches.
    - Identify the cutoff date in your LLM's training data

    Knowing the cutoff date for your model's training data can be helpful in knowing how up-to-date the responses you're receiving from your LLM are.

2. Which of the following best describes how LLMs can be used to support security testing?

    - LLMs are now sophisticated enough to outperform dedicated cybersecurity professionals
    - Assigning a role to the LLM (e.g. as a cybersecurity expert) can often improve the quality of the suggestions provided.

      Assigning a role tailored to the task at hand, in this case a cybersecurity expert, will often yield higher quality results when working with an LLM.

    - LLMs can usually find all potential security flaws in a single pass.
    - LLMs can help brainstorm potential security flaws in your software and suggest solutions that can be discussed with dedicated security professionals.

      LLMs can be a great way to kickstart the process of security testing your software.

3. How can an LLM (like ChatGPT) assist in improving code performance?

    - By deleting portions of code that introduce performance bottlenecks.
    - By optimizing functions when given detailed context and profiling results.
    - By timing your code's execution time to determine whether it is already optimized.
    - By running the code for you and reporting back on observed bottlenecks.

    An LLM can provide valuable optimizations when given detailed context, such as profiling results, enabling it to suggest targeted improvements.

4. What is the primary advantage of automated testing over manual functional testing?

    - It is less reliable than manual testing.
    - It requires more human intervention.
    - It saves time and ensures consistency.
    - It is more prone to human error.

    Automated testing automates repetitive tasks, saving time and ensuring consistent results, unlike manual testing which can be time-consuming and error-prone.

5. What is a key takeaway from using tools like cProfile in combination with an LLM for performance optimization?

    - Profiling results provide valuable context for the LLM.
    - LLMS perform better without the distractions caused by profiling results.
    - Tools like cProfile are no longer necessary once you have access to an LLM to help with performance testing.
    - LLMs cannot improve code performance without the help of profiling results.

    Profiling results give detailed context about performance bottlenecks, enabling the LLM to suggest more effective optimizations.