1. Read the paper on Avoiding the Top 10 Security Design Flaws. The paper is attached here: Top-10-Flaws.pdf

   (a) **Question 1:** List the Top 10 Flaws in your own words, using no more than two sentences per flaw. Note this must be in your own words, no points will be awarded for simply cutting and pasting the text from the paper.

      i. **The first flaw has to do with software that assumes trust in sources that they should not. A simple example is any sort of client that sends data to your system (server). The flaw is that some systems just assume the client is correct and non-hostile.**

      ii. **The second flaw involves leaving holes with authenticating users. An example could be an obscure url in a website that an attacker can access without being forced to first authenticate themselves as a user.**

      iii. **Another flaw is not authorizing a user after authenitcating them. An example is not providing another layer of authentication after a possible attacker (could be in another country) has a user's card and pin and then tries to transfer large sums of money.**

      iv. **The fourth flaw deals with software that should separate data that your system processes and code. When this is ignored, this could lead to simple attacks such as SQL injections where code is inserted where the system expects data and ends up running the code as instructions.**

      v. **The fith flaw is not explicitly validating all data the system handles. Common examples are in web development where input data on forms with get validated or images get sanitzed before moving on in the system.**

      vi. **The sixth flaw handles the inappropriate use of cryptography. Examples of this include using your own algorithm (instead of professional libraries) or making wrong assumptions about how the libraries handle encryptions**

vii. **The seventh flaw includes identifying private / sensitive data and handling it appropriately. This ranges depending on preserving confidentiality, integrity, etc...but an example is the confidentiality of a bank app that uses context to show account information only to appropriate users and not someone who shouldnt have access.**

viii. **The eight flaw talks about how important it is to think about the user. The flaw is some apps make security way too involved for the user and the user might not even care if this specific data is protected or not.**

ix. **The ninth flaw involves understanding the effects of adding external components to your system. One important example that comes to mind is using third party Stripe for dealing with payments. If they have a security breach, then payment information could be leaked and then used on your application or others.**

x. **The last flaw deals with ensuring your system is flexible with future changes. A simple example involves making sure your system has easy methods to replace sensitive information. So keeping API key in a config .env file so if compromised, you only need to switch out that one value instead of tons of uses spread out in code.**

(b) **Question 2:** Pick one of the Top 10 Flaws and describe how code you produced suffered from that flaw. If you believe you have never written any code with one of the Top 10 Flaws, then invent an example (not one of the examples in the paper) that demonstrates the flaw.

I've actually recently introduced the fith flaw into a feature I was building for a client. This client's business (in a nutshell) takes uploaded books from authors and markets them. The client's business heavily relies on Amazon's product API to pull book information to their platform. But amazon randomly cancelled their account which broke their whole system. I had to build a separate uploader that would be a backup when this API failed. A big piece of this was a file uploader that would accept files, sanitize them, and upload the image to gcloud

buckets for storage while returning a public url used to serve on the client side. Being in a rush for this feature, I forgot to include validating on the file types. So anyone could upload any sort of file instead of what should've been only images. This was an easy thing to fix but extremely important to check when it comes to security.

2. **Review Question 16.1** What are the principal concerns with respect to inappropriate temperature and humidity?

   Under higher or lower temperatures (outside the range of $50^{\circ}F - 90^{\circ}F$), computers may not be able to cool or heat themselves adequately and their internal parts may be damaged. Thus either producing undesirable results or putting the machine out of commission.
   Under high or low humidity (outside the range of $40\% - 60\%$), the electronic equipment can be damaged due to corrosion or condensation where circuit shorts could occur. Under low humidity, state electicity could be effected. If a statically charged person or obejct come into contact with the hardware, it could damage sensitive electronic circuits.

3. **Review Question 16.7** List and describe some measures for dealing with power loss.

   In dealing with power loss, there needs to be an uninterruptible power source such as a backup battery unit (UPS). UPS's can function as a surge protector, noise filter, and automatically shutdown devices when battery runs deadly low. For long blackouts (caused by catestrophic events) generators could be used.

4. **Review Question 16.8** List and describe some measures for dealing with human-caused physical threats.

   (a) **Physical contact with a resource is restricted by restricting access to the building where the resource is housed. The point of this is to deny access to outsiders but doesn't address issue of unauthorized insiders / employees.**

(b) **Physical contact with a resource is restricted by putting the resource in a locked room, cabinet, or safe.**

(c) **A machine may be accessed, but it is secured to an object that is difficult to move. This will prevent theft but could allow vandalism or unauthorized access.**

(d) **A security device controls the power switch.**

(e) **A moveable resource is equipped with a tracking device so a sensing portal can alert security personnel or trigger an automated barrier to prevent the object from being moved out of its proper security area.**

(f) **A portable object is equipped with a tracking device so its current position can be monitored continually.**