1. The CIA Triad:

To understand cybersecurity, I first looked at the foundation of all security policies: the CIA Triad. This isn't just about stopping hackers; it's about ensuring three specific things happen with our data.

- **Confidentiality** (Keeping secrets secret): This is about access control. Only the right people should see the data.

- Example: In banking, confidentiality is why I can't simply Google someone else's account balance. Encryption ensures that only the bank and the account holder have access to that financial data.

- **Integrity** (Trusting the data): This ensures that the information hasn't been tampered with or corrupted.

- Example: On social media, integrity is crucial. If I post a photo or a status update, the system must ensure that no one intercepts that post and changes the caption to something offensive before it reaches my friends' feeds.

- **Availability** (Access when needed): Security is useless if the system doesn't work.

- Example: A banking app needs to be online 24/7. If the system crashes (a denial of service) when I need to pay a bill, that is a security failure because the service is no longer "available."

2. Different types of attackers:

I learned that "**hackers**" aren't a single group. They vary wildly in motivation and skill.

- **Script Kiddies**: These are usually unskilled individuals (often younger) who use pre-made tools or scripts found online. They aren't writing code; they are launching attacks for the thrill or bragging rights.

- **Insiders**: These are dangerous because they are already inside the "castle walls." An unhappy employee or a contractor with legitimate access can steal data or sabotage systems without needing to "hack" in.

- **Hacktivists**: These groups aren't in it for money; they are motivated by ideology. They attack organizations to make political or social statements (like defacing a government website).

- **Nation-State Actors**: These are the most dangerous. Funded by governments, they have high resources and skills. Their goal is usually espionage, stealing national secrets, or disrupting the critical infrastructure of other countries.

3. The common Attack Surface:

I explored the concept of an "**Attack Surface**" which is essentially the sum of all the open doors and windows in a digital environment. The more complex an organization is, the larger its attack surface.

• **Web Applications**: Forms, search bars, and login pages are all entry points.

• **Mobile Apps**: The code sitting on a user's phone can be reverse-engineered.

• **APIs**: These are the bridges that let software talk to each other; if they aren't guarded, they leak data.

• **Cloud Infrastructure**: A simple misconfiguration in an AWS bucket can leave terabytes of data open to the public.

4. The Importance of the OWASP Top 10:

The **OWASP Top 10** is the industry standard—a "most wanted" list of security risks. It is critical because it tells developers exactly what the most dangerous and common vulnerabilities are (like Injection attacks or Broken Access Control) so they can prioritize fixing them. It’s essentially a survival guide for web developers.

5. Daily Life Through a Security Lens:

I mapped out the applications I use every day to see where they are vulnerable:

• **WhatsApp**: The attack surface here is the Mobile Device and the Network. While the chats are encrypted, if my phone is stolen (physical access) or infected with malware, the encryption doesn't matter.

• **Banking Apps**: The surface involves APIs and Web traffic. The biggest threat here is usually "Man-in-the-Middle" attacks, where someone on a public Wi-Fi tries to intercept the transaction data.

• **Email**: The surface is Social/Human. The technology works, but the user is the weak link. Phishing emails try to trick the human into giving up the password.

6. Data Flow Analysis:

To understand where attacks happen, I tracked how data moves.

The Flow:

1. **User Input**: I type my password into a phone.

2. **Application**: The app processes the password.

3. **Transmission**: The password travels over the internet.

4. **Database**: The server checks the password against its storage.

7. Where the attacks happen during this flow:

• **At the User**: Keyloggers or shoulder-surfing can steal the input before it's even sent.

• **During Transmission**: If the data isn't encrypted (HTTPS), attackers can "sniff" the packets in transit.

• **At the Database**: SQL Injection attacks can trick the database into dumping all the stored passwords.

8. Summary:

Cybersecurity is fundamentally about managing risk. It starts with the CIA Triad to define what we are protecting. We then have to look at our Attack Surface to see where we are exposed. Whether the threat is a bored Script Kiddie or a sophisticated Nation-State, the goal is the same: to secure the data flow from the user to the database. Tools like the OWASP Top 10 give us the roadmap to close those holes and keep the system secure.

Interview Questions & Answers

Q1: What is the CIA triad?

Ans: It’s essentially the three pillars of security that we try to balance. Confidentiality is about keeping secrets secret—like making sure only I can see my bank balance. Integrity ensures that the data hasn't been messed with or changed by mistake. And Availability just means the system works when you need it to—because the most secure computer in the world is useless if it's turned off.

Q2: What is an attack surface?

Ans: I like to think of the attack surface as the total number of 'doors and windows' a hacker could try to open. It’s everything from a login page on a website to an employee’s weak password. The more complex a system is, the bigger that surface gets, and our job is to keep it as small as possible.

Q3: What is the difference between vulnerability, threat, and risk?

Ans: The easiest way to describe it is with a house. A vulnerability is a broken lock on the front door. The threat is the burglar who might try the door. And the risk is the actual chance of them breaking in and stealing something valuable.

Q4: What are common cyber attackers?

Ans: They really range in skill. You have Script Kiddies, who are basically amateurs using other people's tools for fun. Then you have Insiders, like disgruntled employees, who are dangerous because they already have access. There are Hacktivists, who attack for political reasons, and finally Nation-State Actors, who are government-funded spies looking for highly sensitive data.

Q5: Why is OWASP Top 10 important?

Ans: It’s basically the 'Most Wanted' list for web vulnerabilities. It tells us exactly what the most critical and common security flaws are right now. Developers use it as a checklist to make sure they aren't leaving obvious holes in their code that could lead to a data breach.