Maridelle Gonzales

CS405

7-1 Journal

The video provided a valuable overview of hacker motives and how their behaviors vary depending on their intent. One important takeaway is that while the motive may not always be clear, it’s essential to consider why an attacker would target a system. This helps developers and security teams think like a hacker, anticipate threats, and design more secure applications from the start.

In my own practice, I’ll apply this concept by always assessing the “why” behind potential vulnerabilities. For example, if a piece of code is exposed to user input, I’ll ask myself: What could an attacker gain by exploiting this? Thinking in terms of motives helps me prioritize security measures, especially when deciding what to secure first based on risk and reward. It also helps guide logging, monitoring, and alerting strategies.

If I were explaining this concept to a new developer on my team, I’d tell them that understanding a hacker’s motive is like understanding your opponent’s strategy in a game of chess. It’s not just about fixing bugs as it's about anticipating where and how someone might try to break the system. I’d encourage them to ask: Who might want to break this? What would they gain? and How easy is it to do?

One example I’ll include in my final reflection in Module Eight is how motive connects directly to Zero Trust. If we assume that no one should be trusted by default, regardless of their location or credentials, we’re already thinking with a security-first mindset. Recognizing that threats can come from anywhere, even insiders, helps reinforce why policy enforcement, logging, and least privilege access are so critical.