# Journal: Consider the Motive for the Attack

Understanding the motive behind a cyberattack is not always straightforward, but I believe it's one of the most important practices in secure coding. By anticipating why an attacker might target a particular system or application, I can take proactive steps to secure my code and minimize vulnerabilities that could be exploited for financial gain, data theft, sabotage, or even reputation damage.

In my own practice, I apply this concept by constantly asking myself: 'If I were an attacker, what would I target?' This mindset helps me identify weak points in logic, input handling, authentication, and data storage. For instance, when I’m designing login systems, I don’t just think about whether it works I think about how someone could abuse it. Would they try a brute-force attack? Could they inject malicious code? This approach shapes how I choose encryption, validate inputs, and structure permissions.

If I were mentoring a new developer on my team, I would explain it like this: 'Attackers are like detectives but with bad intentions. They look for clues in our code to figure out where they can get in or what they can exploit. If you can think like them, you can stay one step ahead.' I’d encourage them to do regular code reviews with a security-first mindset and always ask themselves what the attacker’s motivation could be. That alone can shift how we prioritize risks and how much effort we invest in hardening different parts of the system.

One example of this concept that I plan to use in my final Module Eight reflection is the risk posed by insufficient input validation in user forms. If an attacker is motivated by data exfiltration or injecting malware, they might exploit a form field to execute cross-site scripting or SQL injection. By understanding that motive, I now write code that strictly sanitizes and validates all input, assuming every field could be a potential attack vector.

Ultimately, secure coding is not just about writing correct code it's about writing resilient code. And resilience comes from anticipating the motive of those who want to break it.

**References**

TED. (2018, October 2). The 1s and 0s behind cyber warfare [Video]. YouTube. <https://www.youtube.com/watch?v=BoWouwPGtVY>