**Julio Pochet – 06/05/2025**

**Module 2.1 – Discussion Board  
  
Use and Abuse Case Breakdown**

For this discussion, I reviewed the use case diagram from the module that outlines common system tasks—logging in, creating, updating, deleting, printing records, and logging out. These seem routine at first, but once you start thinking about how someone could misuse them, the risks really start to show.

Here’s how I broke it down:

* **Login** – Normally just entering your credentials, but an attacker might use brute-force scripts, steal session tokens, or trick users into handing over info (like through phishing).
* **Create Records** – This could be adding a client file, but abuse might involve SQL injection, flooding the system with fake records, or slipping in entries with hidden privileges.
* **Update Records** – A user might fix or change data, but a malicious user could alter logs, insert conflicting info, or make unauthorized updates to manipulate outcomes.
* **Delete Records** – Intended for clearing old or incorrect data, but it could be abused to erase important records, wipe logs, or perform bulk deletions that cause damage.
* **Print Records** – A legit use might be printing a report, but someone could print private info without permission or intercept print jobs across the network.
* **Logout** – This should end a session, but it’s risky if the session stays active or is hijacked. Some systems might even be tricked into thinking a user logged out when they didn’t.

I created a diagram to go along with these use/abuse cases. Feedback is always welcome!

A screenshot of a chat

AI-generated content may be incorrect.