**Julio Pochet – Module 9.1 Discussion: Bug Tracking**

When it comes to tracking bugs, especially ones that affect security, the system you use really matters. If I were on George Everett’s team at MeCo, I’d recommend starting with a **shared bug tracking spreadsheet or moving into a tool like Trello or Jira**, depending on how complex the workflow gets.

To keep things organized, every bug should include:

* **Date Found**
* **Bug Description**
* **Severity** (Low, Medium, High, or Critical)
* **Assigned Developer**
* **Status** (Open, In Progress, Resolved)

While whiteboards and sticky notes might work in a startup environment, they don’t scale well or support remote teams. A spreadsheet (like Google Sheets or Excel) is a solid starting point because it's easy to use, shareable, and allows for sorting/filtering by severity or status. It also works well when exporting for reporting or auditing.

I created a visual example of how this setup could look. It includes both **code bugs** (like broken functions or UI errors) and **security bugs** (like XSS or session handling issues), which helps the team prioritize what really needs attention fast.

📄 Visual Example:

A screenshot of a tracking example

AI-generated content may be incorrect.

For MeCo, this system keeps things simple while still being effective and easy to upgrade as the team or codebase grows.

**Question for classmates**: Would you prefer to keep security bugs tracked in the same system as code bugs, or do you think they should be isolated in a separate log for privacy and compliance reasons?