Next in Sprint V2.1 (E2E Round-Trip)

Now we move from “can I talk to OpenAI?” → “can PromptForge do the full round trip with Channels A & B.”

Here’s the plan, in order:

1. **Environment Sentinel**

   - I’ll add `docs/environment.md` and wire that into SYSTEM rules so the models always see: *Windows 11, PowerShell 7, Python 3.12, ODBC 18 — no bash/zsh — full files only, no diffs.*

   - You’ll see a “Show Effective Rules” button confirm it.

     is there a way to add parsing and lexical analysis to every proposed code or command line received from the AI or proposed as a prompt for submission. in other words if the AI gives me a command line or a piece of code I would like to pre process it and hand it right back to the AI saying you are not in compliance with our shell 7 or Python 3.12 odbc etc

     The same thing can happen after preparing a response or a prompt that it's not in compliance by either prompt Forge or perhaps yours or my editing in preparation for a submission I don't want it to pass compliance if it can't meet basic environment rules

     I want everything submitted for my approval to go through compliance review. so ideally there would be no situation where something comes to me and is not in compliance with our base environment and if it's not in compliance kick it back.

2. **Channel A (code/JSON) test**

   - I’ll mock up a tiny “acceptance file” (like a toy `.py` with a bug).

     That's a good start but I can give us some pretty realistic problems in short order. I've got several projects going on right now in each one of them is bringing up bugs what I'd like to add to the existing application is a project

System wide vs Project specific content:

tLet's add project table to this system that will have a drop down that we can identify which project were working on and so basically every field in the application would be project dependent we may have common systems wide rules across all of them but there may be specific rules for specific projects for example odbc may be only relevant to projects where we're using that database technology and so each project would have a set of defaults However we were able to share scenarios across multiple projects each project would have a unique project root the projects would have unique tasks and content on the prompt rules would have system wed rules but it's possible to have project specific rules as well sentinels would be typically systemwide but I can envision allowing for project specific sentinels same with output contract so all the fields in those tabs scenarios would be system light but also some that could be project specific the history would be project specific the settings The settings would be default a system-wide but project specific And the help would be system wide

- We'll send it through Call A → Validate → Apply → Undo.

  OK

- Goal: see the file modified and then restored.

  OK

3. **Channel B (prose) test**

   - Same run, but ask for explanation. OK
   - Verify Call B returns a clear prose reply alongside A. I am not sure how the system can verify that the pros are clear that's going to require human interpretation did you have something else in mind here that I'm not thinking about

4. **Graceful API errors**

- Simulate bad key/quota (e.g., rename `.env` temporarily) and confirm you see the friendly banner, not a crash stacktrace.

  Right now the error messages are beingWritten to the prompt review files parsed prose errors it's a overloaded field and I think in a workflow I envision it like this the files parsed would be files that I would copy and paste back into the AI after its gone through validation the prose is a separate text boxed that comes from the AI that's for human consumption and I don't think they should be commingled with in the same text box. likewise the errors need to be separated because oftentimes they will require a separate type of submission in fact typically what I would envision is after an error comes back it may be sent back to the AI with a question so keeping them in separate text boxes will be necessary so break that out please

5. **Tooltips + Dry Run**

   - You should see hover tooltips (JSON-driven) and be able to paste a JSON payload into Dry Run without hitting OpenAI.

     I am not sure why you have tool tips and dry run under the same topic here tooltips is for help on each one of the fields and I am not sure what dry run is all about so I've you need to explain that In terms of json driven tool tips I understand that's a very good way of being able to manage content like this because once it's written it'll probably be static but it's not reasonable to expect a human being to write json I can imagine using an AI to say edit this particular content around a given field and having the AI update correct if the content I don't want to over engineer this so for now let's just say that in the editing to the json will be directed through an AI and just replace as edits are needed

---

What I need from you now

Can you give me a **tiny “acceptance file”** we can use for Channel A?

- For example, a 10-line Python file with a simple bug (e.g., `print("Hello` missing quote).

- Or a PowerShell snippet with a typo.

Something small and controlled is best, since this is just to prove the pipeline.

Do you have one in mind, or do you want me to generate a starter buggy file for us to run through?

Here's a bug I'm working on on the PortifolioAI project

```
(.venv) PS G:\My Drive\Code\Python\Portfolio-AI-Lab> & "G:\My Drive\Code\Python\Portfolio-AI-Lab\.venv\Scripts\Activate.ps1"
                                        python tools/prod_ui.py
>>
C:\Users\Owner\AppData\Local\Programs\Python\Python312\python.exe: can't open file 'G:\\My Drive\\Code\\Python\\Portfolio-AI-Lab\\tools\\prod_ui.py': [Errno 2] No such file or directory
(.venv) PS G:\My Drive\Code\Python\Portfolio-AI-Lab> python tools\prod_ui.py
>>
C:\Users\Owner\AppData\Local\Programs\Python\Python312\python.exe: can't open file 'G:\\My Drive\\Code\\Python\\Portfolio-AI-Lab\\tools\\prod_ui.py': [Errno 2] No such file or directory
(.venv) PS G:\My Drive\Code\Python\Portfolio-AI-Lab> pip list
Package         Version
--------------- -------
colorama        0.4.6
loguru          0.7.3
numpy           2.3.3
pandas          2.3.2
pip             25.2
pyodbc          5.2.0
python-dateutil None
python-dotenv   1.1.1
pytz            2025.2
tqdm            4.67.1
tzdata          2025.2
wheel           0.45.1
```

```
win32_setctime  1.2.0
(.venv) PS G:\My Drive\Code\Python\Portfolio-AI-Lab>
```