

Forum:[Hack Forums](#)

Thread: [AI Pentest Tutorial](#)

blood69sucker - August 21, 2026, 12:39 pm

I've been experimenting with FastAPI and Ollama to simulate a white-hat security agent backend. The workflow includes reconnaissance, vulnerability analysis, and reporting. One useful trick: set "stream": false in Ollama's API calls to avoid JSON parsing errors. This setup helps me test my own websites safely before adding sensitive features like payment systems. Has anyone else tried combining AI with security workflows?

01001 - August 22, 2026, 8:27 am

Sounds interesting, as I've tried building my own set of templates which leverages all the frameworks to assess AI based applications. Although when you say workflows, are you referring N8N?

desmondo - August 22, 2026, 12:55 pm

(Aug 21, 2026 12:39 PM)blood69sucker Wrote: [\[CITE\]](#) I've been experimenting with FastAPI and Ollama to simulate a white-hat security agent backend. The workflow includes reconnaissance, vulnerability analysis, and reporting. One useful trick: set "stream": false in Ollama's API calls to avoid JSON parsing errors. This setup helps me test my own websites safely before adding sensitive features like payment systems. Has anyone else tried combining AI with security workflows? Which local model do you use?

psycheuser - August 22, 2026, 4:56 pm

Solid setup mate. Setting stream to false saves a lot of headaches with JSON parsing when you are automation testing. Personally prefer using LangChain or just custom python scripts over N8N for linking the recon tasks together, gives better control over the agent. Safe testing before payment integrations is definitely the way to go.

los911 - August 27, 2026, 4:01 am

I keep finding Qwen hallucinating vulnerabilities

rspower - October 15, 2026, 6:24 am

Here is a tool for Windows for automatic pen testing websites with local ai
<https://github.com/SLP-DEV1/PenX>