

Name - Shubham Yadav

### Terminal Output :

PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL PORTS + ⌂ ⌄ ⌁ X

```
Enter user_id: pawan
You: Malicious Python script executed
AI (pawan): Previous issues found: An alert was issued for a malicious Python script execution on Host LAB-07 (Incident #006). The incident was resolved by stopping the script, performing malware analysis, and cleaning the environment.
Suggested fix: Perform a thorough scan of the Host LAB-07 to ensure no residual threats remain
.
Severity: High Alert
Structured Output: {
  "response": " Previous issues found: An alert was issued for a malicious Python script execution on Host LAB-07 (Incident #006). The incident was resolved by stopping the script, performing malware analysis, and cleaning the environment.\nSuggested fix: Perform a thorough scan of the Host LAB-07 to ensure no residual threats remain.\nSeverity: High Alert",
  "extracted_entities": {
    "Severity": "High"
  }
}

Enter user_id: █
```

The terminal output shows a malicious Python script execution alert for user\_id pawan. It includes AI analysis, suggested fixes, and structured output JSON.

```
Enter user_id: shubham
You: Multiple failed SSH logins
AI (shubham): Previous issue found: Multiple failed SSH logins have been detected on SRV-LNX-01 in Incident #001.

Suggested fix/solution: Block the source IP (10.1.1.9), reset the password, and enable Multi-Factor Authentication (MFA).

(Severity: HIGH ALERT)
Structured Output: {
  "response": " Previous issue found: Multiple failed SSH logins have been detected on SRV-LNX-01 in Incident #001.\n\nSuggested fix/solution: Block the source IP (10.1.1.9), reset the password, and enable Multi-Factor Authentication (MFA).\n\n(Severity: HIGH ALERT)",
  "extracted_entities": {
    "IP": "10.1.1.9"
  }
}

Enter user_id: █
```

The terminal output shows multiple failed SSH logins for user\_id shubham. It includes AI analysis, suggested fixes, and structured output JSON. A cursor is shown at the end of the input line.

## FastAPI :

The screenshot shows the FastAPI documentation interface. At the top, it displays "FastAPI 0.1.0 OAS 3.1" and a link to "openapi.json". Below this, under the "default" section, there are three API endpoints listed:

- POST /ask/** Ask Query
- POST /history/** Get History
- GET /** Read Root

Below the endpoints, there is a section titled "Schemas" which is currently collapsed.

## Streamlit :

The screenshot shows the Streamlit application interface for the "Incident RAG Investigation System". On the left, there is a sidebar titled "Enter your Details" with fields for "User ID" (containing "pawan") and "Question" (containing "Multiple failed SSH logins"). A "Clear History" button is also present. On the right, the main area has a title "Incident RAG Investigation System" with a lightbulb icon. It includes a welcome message: "Welcome to your virtual IT support assistant! Please enter your User ID and *Incident-related question\** below to get instant support." Below this is a "Conversation History" section with a speech bubble icon and a button labeled "Ask". A progress indicator "Analyzing your request..." is shown. At the bottom, a footer note states "Powered by Streamlit, FastAPI, and OpenAI's GPT".