**V1 – how to use + next iteration**

Link to challenge: <https://app.hackthebox.com/challenges/Flag%20Command>

**Step by step:**

1. to start the challenge press “start instance” this will then provide a Host IP
2. while this is running, open the project terminal in chosen IDE and enter “streamlit run GUI/v1\_UI.py”
3. This will then open a streamlit browser where you enter the Host IP given to you earlier
4. After, press “get flag” this runs the self-titled function which returns the flag value to you, completing the challenge.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

This works by the get flag function taking the host parameter from the user input and constructing predetermined http endpoints from it such as:

Target URL = <http://host/api/options>

Flag submit URL = <http://host/api/monitor>

The first URL created contains a Json which stores the “secret” command (a key to get the flag) this is then extracted and submitted in the second URL which receives the secret and returns the flag if correct.

A screenshot of a computer code

AI-generated content may be incorrect.

“/api/options” endpoint json containing “secret” value

**What our next iteration may look like:**

* Currently each api endpoint is manually discovered and checked for the secret. This can be changed so an LLM can check each endpoint for the key.
* in this game the key is also conveniently named secret, this can be changed so an LLM reads all commands and predicts the most likely the key**.**
* Try on a harder challenge which involves using docker kali linux