**CTF Topic: Vulnerability Disclosure Programs Using "YesWeHack VDP Finder" Extension**

**1. Introduction**

"YesWeHack VDP Finder" is a Chrome extension designed to help users find Vulnerability Disclosure Programs (VDPs) for websites. This Capture the Flag (CTF) scenario introduces beginners to the basics of using the "YesWeHack VDP Finder" extension to identify if a given webpage has an associated VDP.

**2. Tools and Requirements**

YesWeHack VDP Finder Chrome Extension: An extension for Google Chrome that helps in identifying Vulnerability Disclosure Programs for websites.

**3. Scenario**

In this scenario, you will use the "YesWeHack VDP Finder" extension to analyze the webpage for GitHub. Your tasks include identifying key pieces of information related to Vulnerability Disclosure Programs and capturing flags based on the analysis.

**4. Process to follow while performing CTF**

Step 1: To start, install the "YesWeHack VDP Finder" extension from the Chrome Web Store or open the link provided to you:

<https://chromewebstore.google.com/detail/yeswehack-vdp-finder/jnknjejacdkpnaacfgolbmdohkhpphjb>.

Step 2: Use this extension to analyze the provided webpage and solve the challenges to capture the flags.

**Questions and Answers**

Flag 1: Presence of VDP

Task: Use the "YesWeHack VDP Finder" extension to check if the GitHub webpage has a Vulnerability Disclosure Program.

URL: <https://github.com/>

Question: Does the GitHub webpage have a Vulnerability Disclosure Program?

Hint: Use the extension to check for the presence of a VDP.

Answer: Yes

Flag Captured.

Flag 2: URL of VDP

Task: Use the "YesWeHack VDP Finder" extension to find the URL of the VDP for the GitHub webpage.

URL: <https://github.com/>

Question: What is the URL of the Vulnerability Disclosure Program for the GitHub webpage?

Hint: Use the extension to find the VDP URL.

Answer: <https://securitylab.github.com/>

Flag Captured.

**Hint**