## **Phishing Awareness in Cybersecurity**

## **Objective :**

* The main objective of this phishing awareness task is to understand how phishing attacks are created and executed, so that their techniques can be recognized and defended against in real-world scenarios. The activity aims to increase awareness about social engineering tactics, fake login pages, and data theft methods commonly used by attackers. By simulating phishing attacks in a controlled environment, participants gain practical knowledge on identifying phishing attempts, reporting them correctly, and implementing preventive measures to strengthen system and user security.

## **Scope :**

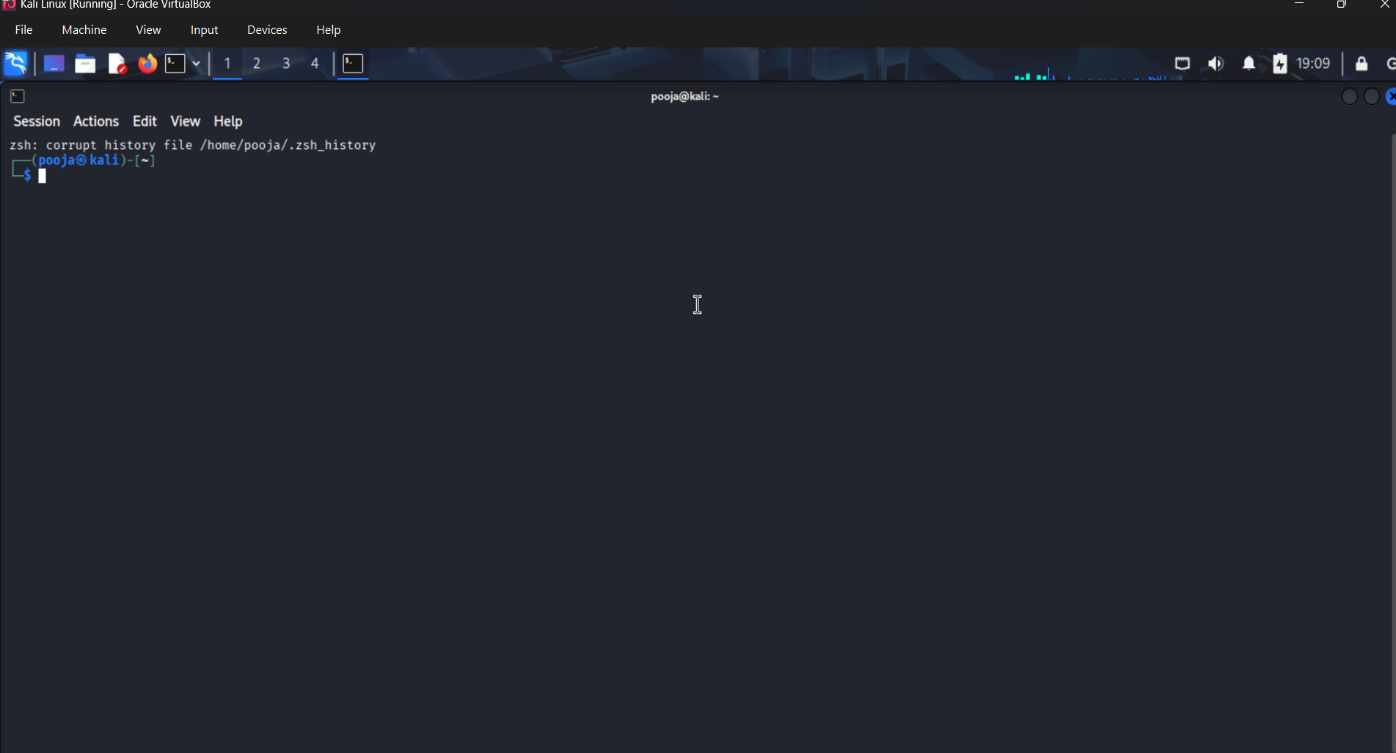
* This task focuses on demonstrating phishing techniques using the **Zphisher** tool in a **safe, authorized, and isolated environment**. The scope includes setting up phishing templates, understanding how attackers clone legitimate websites, and analyzing how user credentials could be captured if proper awareness and protections are not in place. The exercise is strictly limited to educational and research purposes, ensuring no real user data or external systems are targeted. It helps learners understand the working process of phishing tools so they can develop effective countermeasures, strengthen defenses, and educate others on avoiding such attacks.

## **Tools used :**

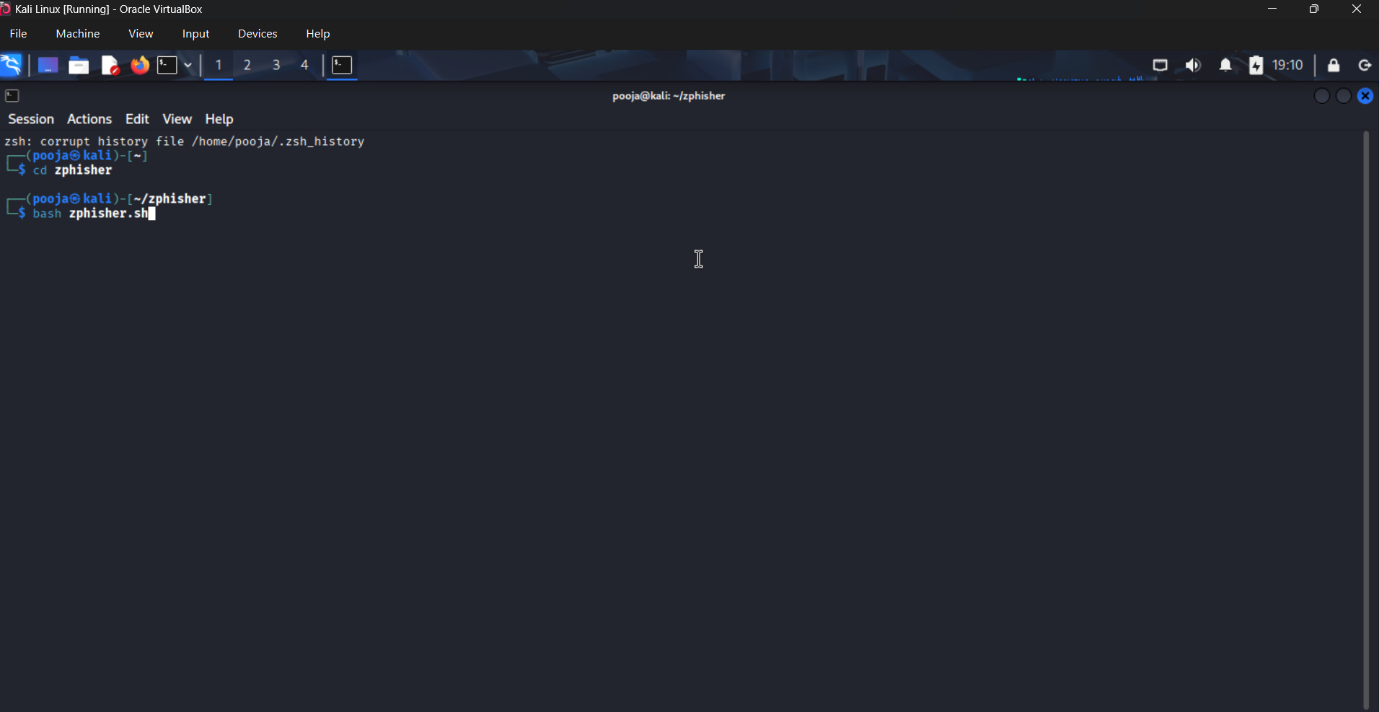
* The primary tool used was **Zphisher**, an open-source phishing toolkit utilized in a controlled virtual lab to demonstrate how phishing pages are created.

## **Timeline :**

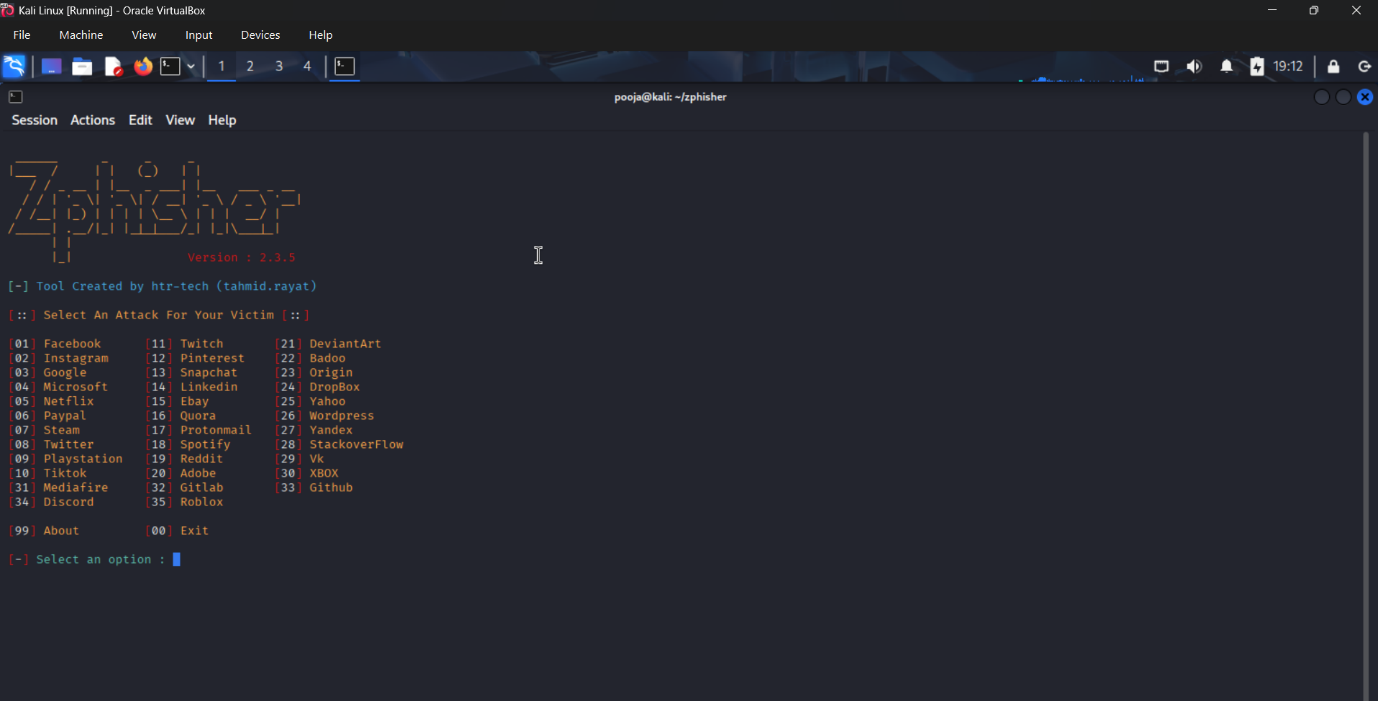
## **1. Opening terminal in kali linux**



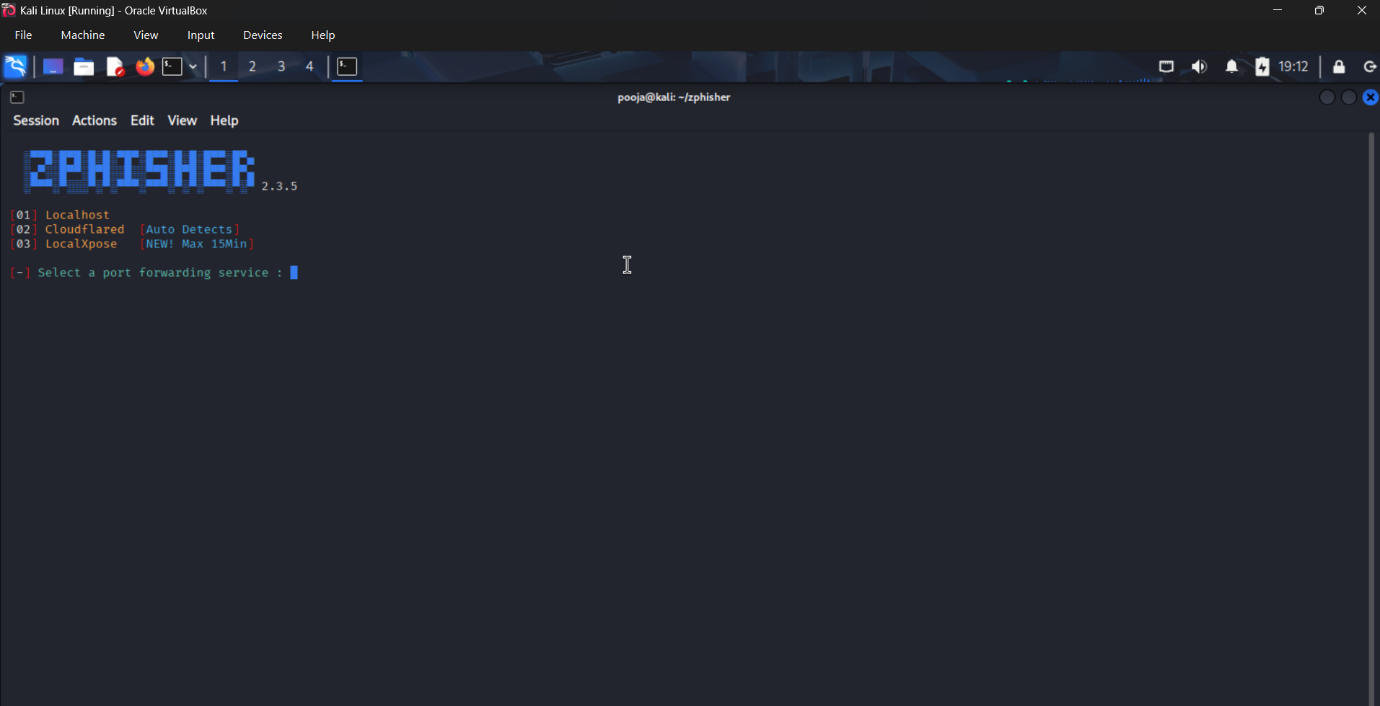
## **2. Change directory to zphisher**



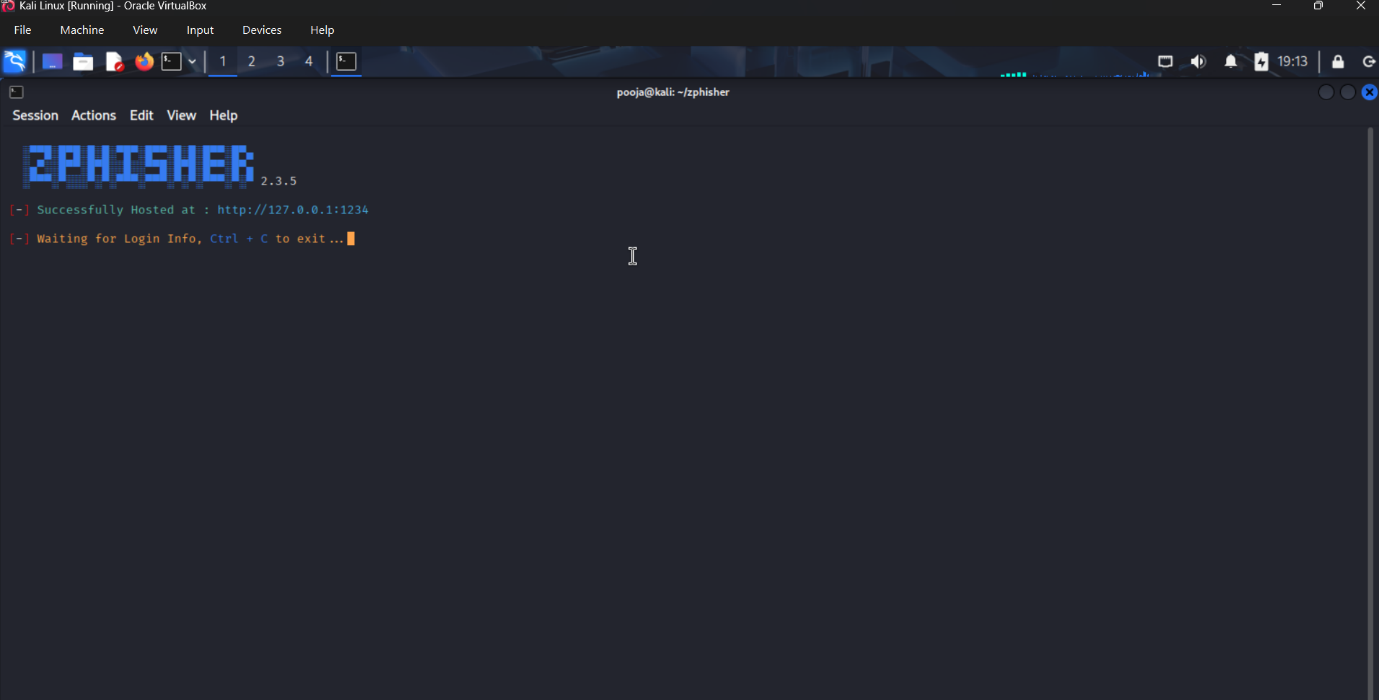
## **3. Starting zphisher and selecting template**



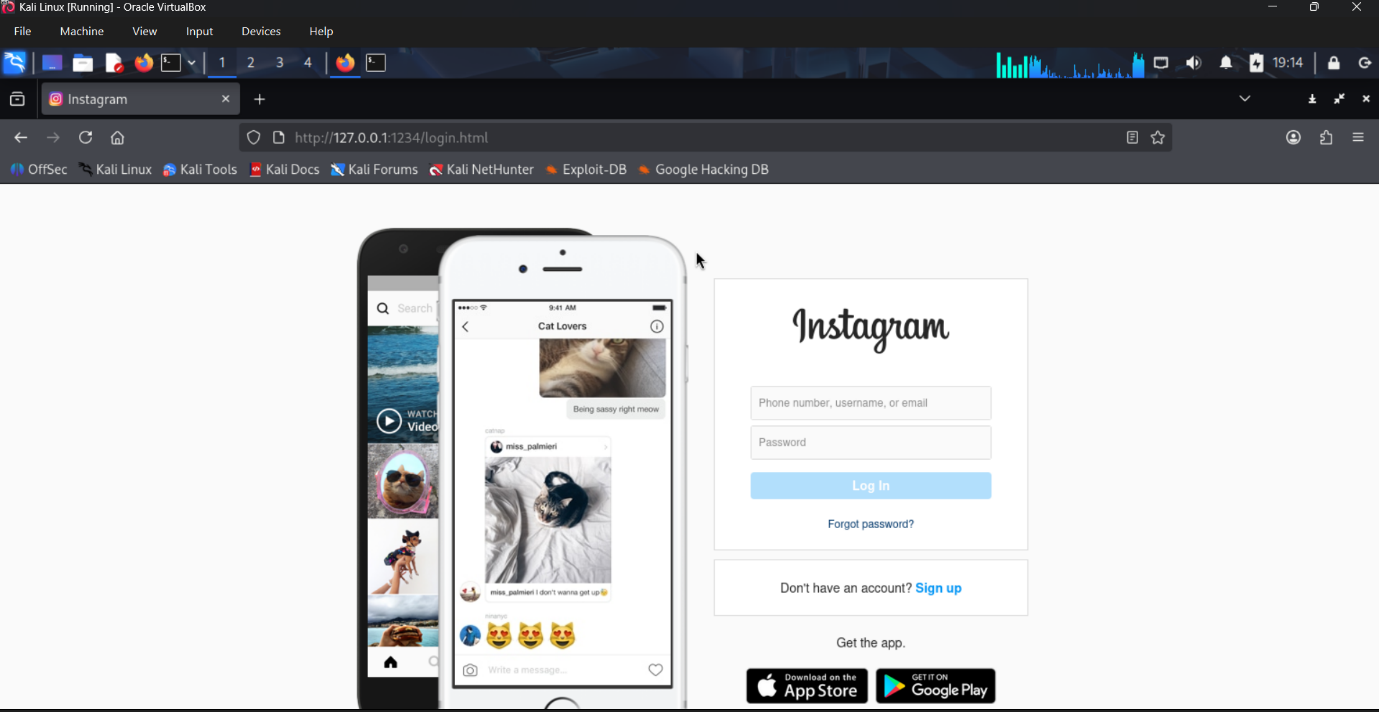
## **4. Selecting phishing method**



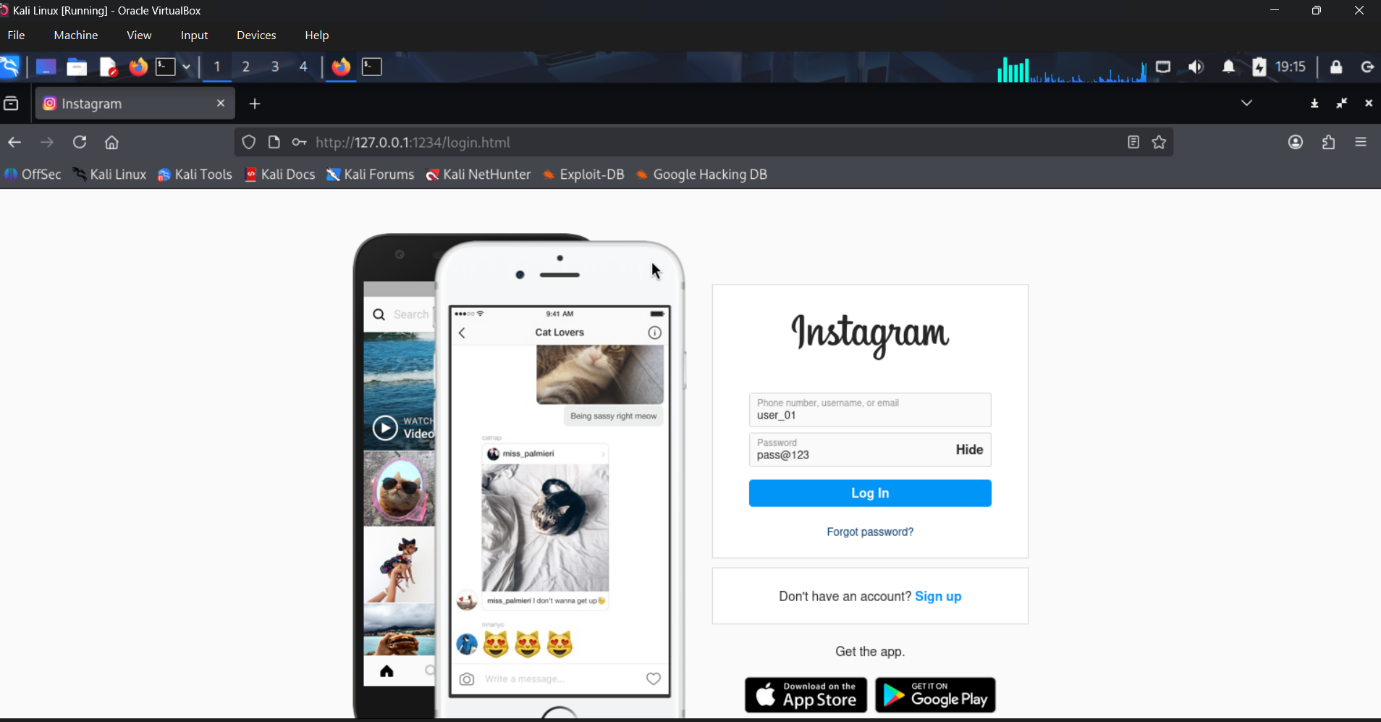
## **5. Customizing phishing URL**



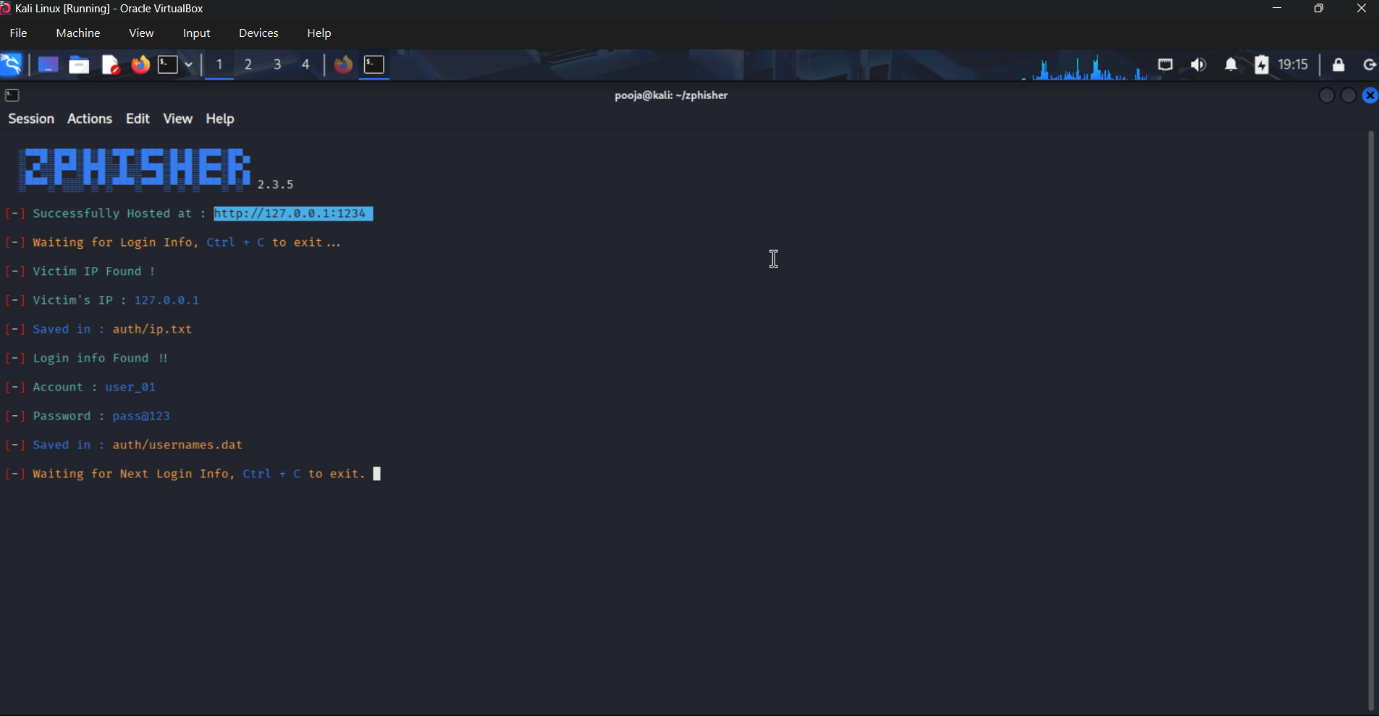
## **6. Fake phishing site deployed**



## **7. User entering credentials**



## **8. Successfully collected user credentials**



## **Conclusion :**

Ways to avoid Phishing:-

* + Verify email senders and website URLs before clicking links.
  + Avoid sharing passwords or personal information online.
  + Enable multi-factor authentication for added security.
  + Keep software and browsers updated.
  + Be cautious with email attachments and links.
  + Use spam filters and security tools.
  + Stay informed about phishing techniques.