Understanding Phishing Attacks:

Disclaimer: This document is written only for educational and awareness purposes. I explored phishing techniques to understand how attackers trick people, so that users can better protect themselves online. This content does not encourage illegal activities.

1. Why I explored phishing?

Phishing is one of the most common cyber attacks today, especially on social media platforms. I chose this topic to understand how normal users are fooled so easily and what mistakes they make while using the internet. My goal was to learn how phishing works so I can help others stay safe online

2. What is phishing in general?

Phishing is a type of online scam where attackers create fake websites that look real. These fake websites are designed to trick users into entering their usernames and passwords. Most people do not notice small differences in website links, which is why phishing is effective.

3. Consequences of Phishing Attacks

- Personal accounts can be hacked.
- Private messages and photos can be misused.
- Financial loss can occur if banking details are linked.
- Hacked accounts can be used to scam others.

4. Tool I Explored for Learning Purposes

For my learning, I explored a phishing tool called Zphisher. I did not use it to attack anyone, but only to understand how such tools work and how attackers think when targeting victims.

5. Observing Tool Interface

In the following screenshot, the tool is opened in the terminal. It shows a list of popular platforms like Facebook. This shows that attackers usually target famous websites because users already trust them. Then, I selected Facebook with a traditional login page.

6. Link Generation

After that, a fake website link is generated. This link can be shared with victims through messages or social media. At first glance, the link looks normal, but it is not the real Facebook website.

Here , I use option 2(cloudFlared) for port forwarding which will work anywhere in the internet.

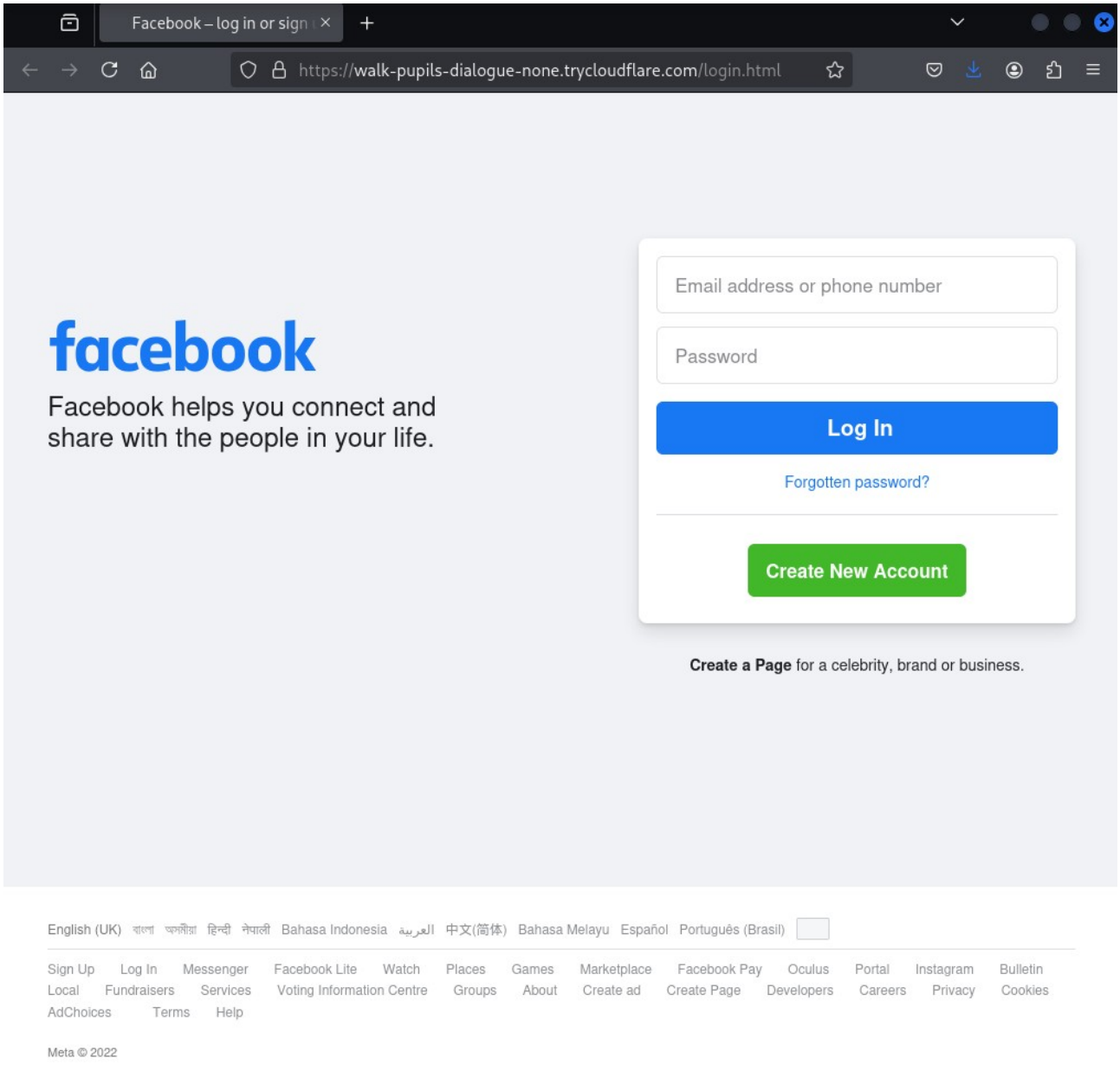
Here, Fake URLS are generated with cloudFlared but only URL 1 worked.

7. What Happens When a Victim Clicks the Link?

When the victim clicks the link, the tool immediately shows activity on the attacker's side like capturing victim's ip address, even before any information is entered.

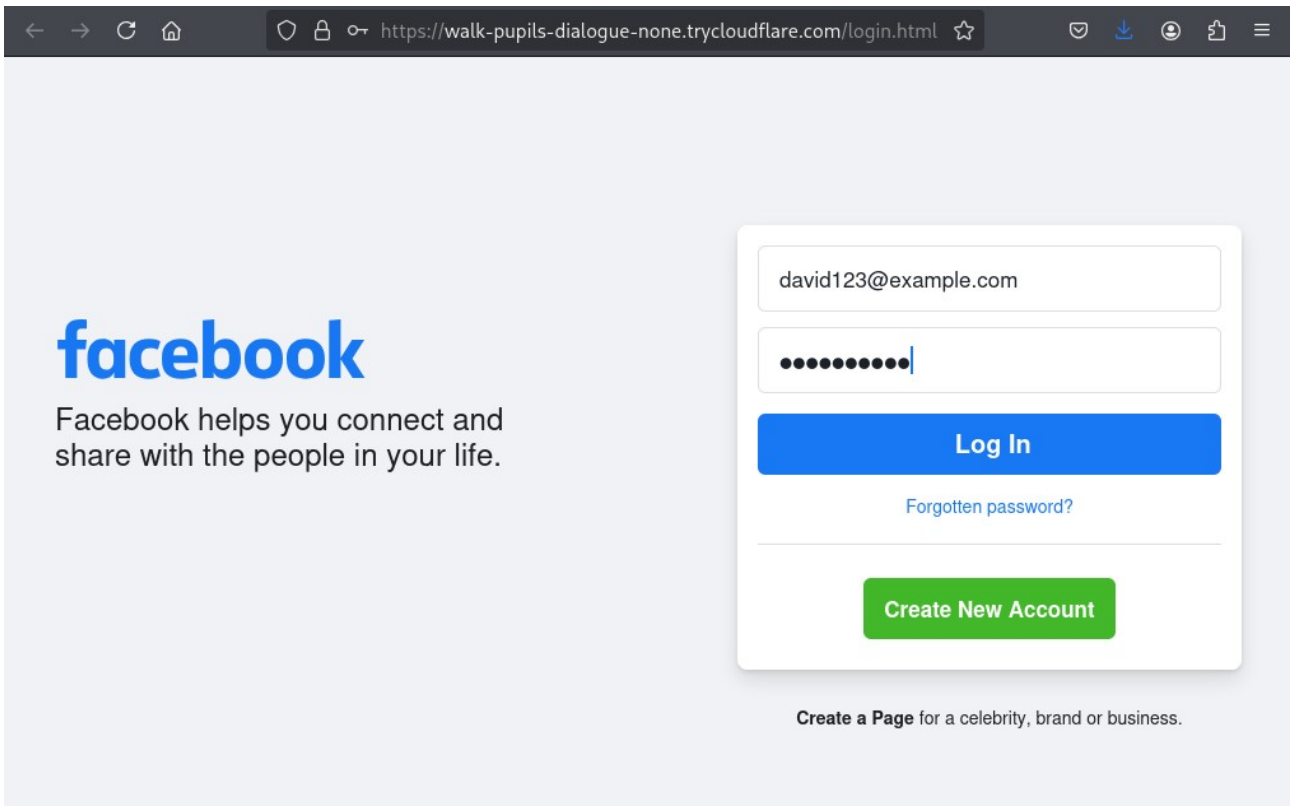
8. Fake Login Page

After clicking the link, it shows the fake Facebook login page on victim's side. It looks exactly like the real one, except for the website link. Most users focus on the page design and ignore the URL, which is why phishing attacks succeed.



9. Capturing Login Details

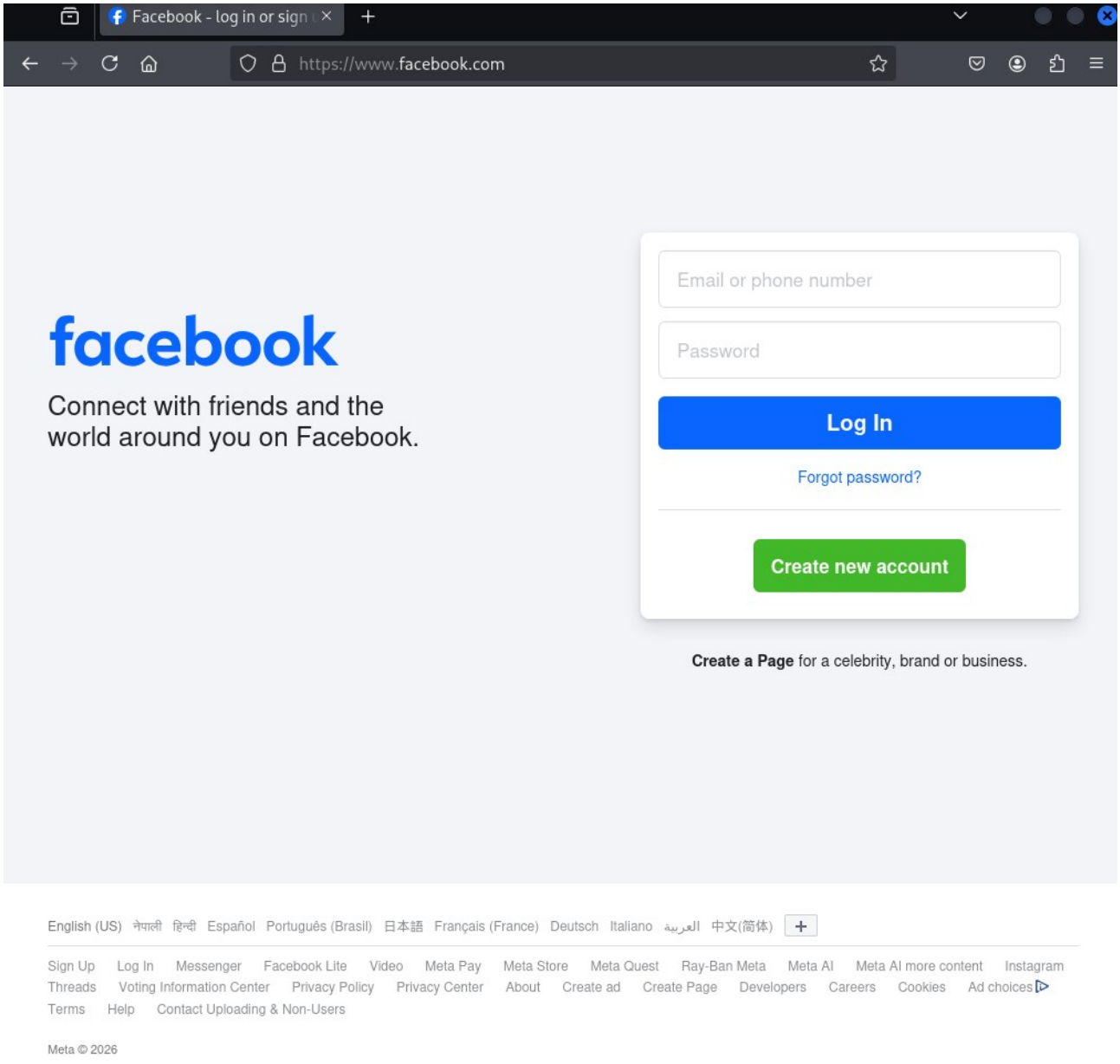
After the victim enters their username and password, the tool displays this information on the attacker's screen. This shows how dangerous phishing can be ,as sensitive information can be stolen within seconds.


https://walk-pupils-dialogue-none.trycloudflare.com/login.html
facebook
Facebook helps you connect and share with the people in your life.
david123@example.com
Log In
Forgotten password?
Create New Account
Create a Page for a celebrity, brand or business.


2PHISHER 2.3.5
[-] URL 1 : https://walk-pupils-dialogue-none.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://blue-verified-badge-for-facebook-free@
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP :
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : david123@example.com
[-] Password : david12345
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.

10. Redirection to the Real Website

After entering the credentials, the victim is redirected to the real Facebook website. This makes the victim think that everything is normal and reduces suspicion.



11. How We Can Protect Ourselves

- Always check the website link before logging in.
- Do not click suspicious links sent by unknown people.
- Use two-factor authentication whenever possible
- Be careful even if the page looks familiar

12. What I Learned from This Exploration

Through this exploration, I learned that phishing attacks do not depend on advanced hacking. They mainly depend on human mistakes and trust. This experience helped me understand the importance of user awareness in cybersecurity.