

FINAL LAB PRACTICE

14/4/2025

Task:

Create and test a phishing website using XAMPP. You must capture login credentials and redirect the user to a fake loading page.

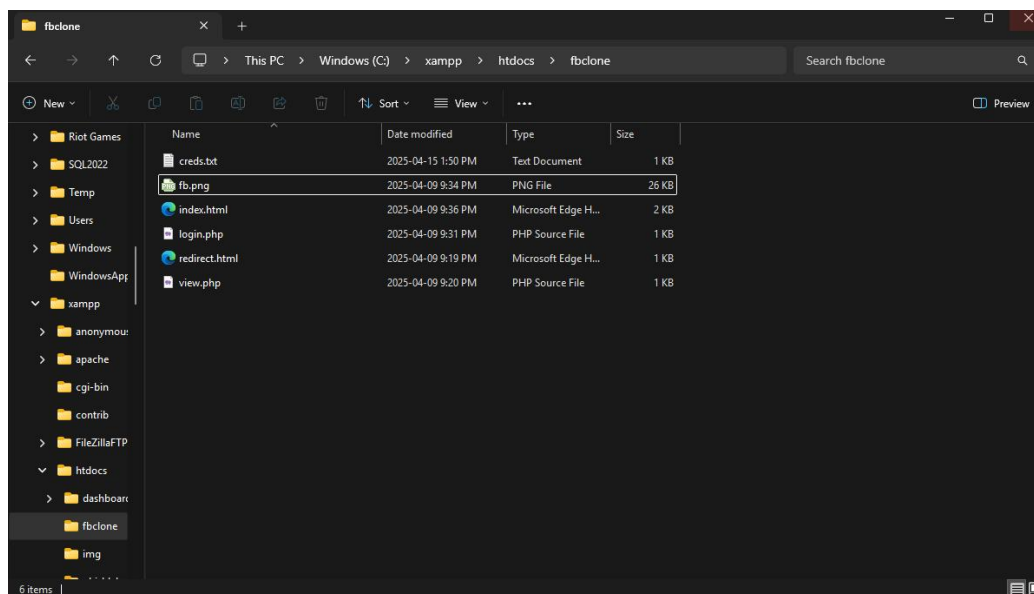
Step-by-Step Instructions:

1. Create Your Project Folder

- Name the folder fbclone
- Place it inside C:\xampp\htdocs

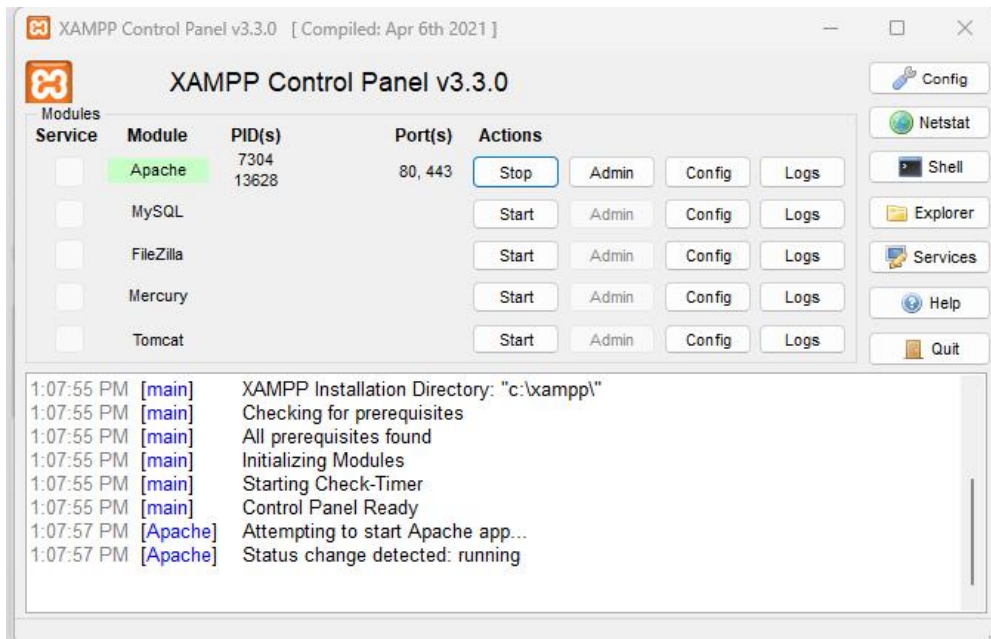
2. Inside fbclone, create the following files:

- index.html – Fake Facebook login page
- login.php – Handles form submission and writes credentials to a file
- redirect.html – A fake redirect page (e.g., “Loading...” or “Connecting...”)
- view.php – Displays captured login credentials
- creds.txt – Leave this blank; it will store captured usernames and passwords
- fb.png – Facebook logo for realism



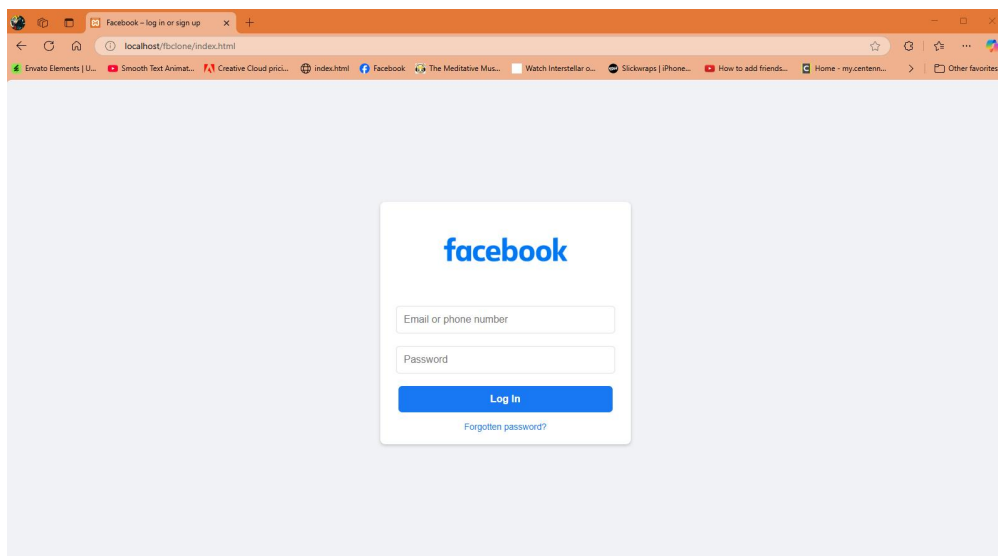
3. Start XAMPP

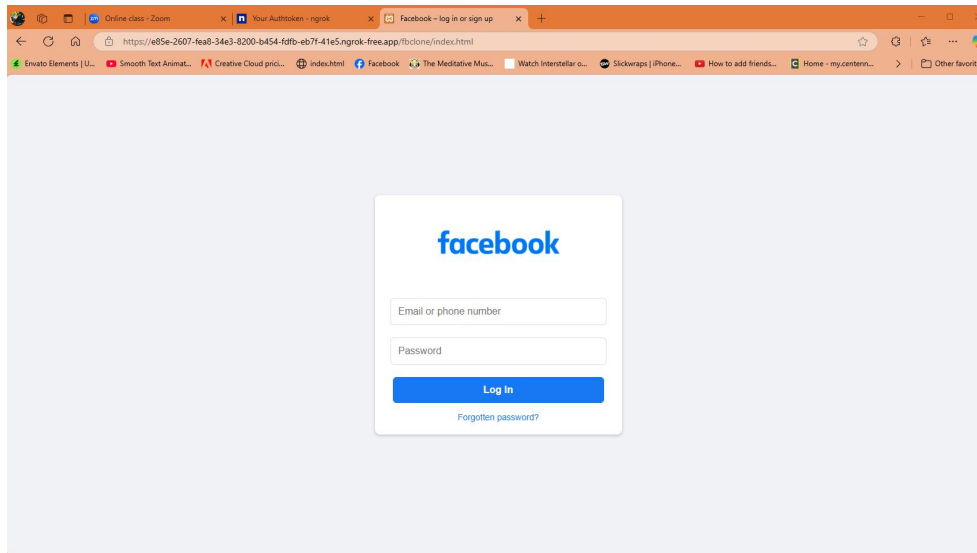
- Open **XAMPP Control Panel**
- Start the **Apache** module only
- Confirm it shows “Running” in green



4. Test on Browser

- Go to <http://localhost/fbclone/index.html>
- Enter any test credentials (e.g., dummy email and password)
- After clicking **Log In**, you should land on [redirect.html](#)
- Visit <http://localhost/fbclone/view.php> to confirm the captured data





5. Use Ngrok to Share Your Site (Bonus Task)

- Open **Command Prompt**
- Navigate to your XAMPP htdocs directory or just run:

nginx

ngrok http 80

- Copy the public HTTPS link generated by ngrok
- Test the phishing site from another device or browser tab
- Credentials from remote submissions will still be stored in creds.txt

```
C:\Users\elure\Desktop\XAMPP X + v
USAGE:
  ngrok [command] [flags]

COMMANDS:
  config      update or migrate ngrok's configuration file
  http        start an HTTP tunnel
  tcp         start a TCP tunnel
  tunnel      start a tunnel for use with a tunnel-group backend

EXAMPLES:
  ngrok http 80                                # secure public URL for port 80 web server
  ngrok http --url baz.ngrok.dev 8080          # port 8080 available at baz.ngrok.dev
  ngrok tcp 22                                  # tunnel arbitrary TCP traffic to port 22
  ngrok http 80 --oauth=google --oauth-allow-email=foo@foo.com # secure your app with oauth

Paid Features:
  ngrok http 80 --url mydomain.com              # run ngrok with your own custom domain
  ngrok http 80 --cidr=allow 2600:8c00::a03c:91ee:fe69:9695/32 # run ngrok with IP policy restrictions
  Upgrade your account at https://dashboard.ngrok.com/billing/subscription to access paid features

Upgrade your account at https://dashboard.ngrok.com/billing/subscription to access paid features

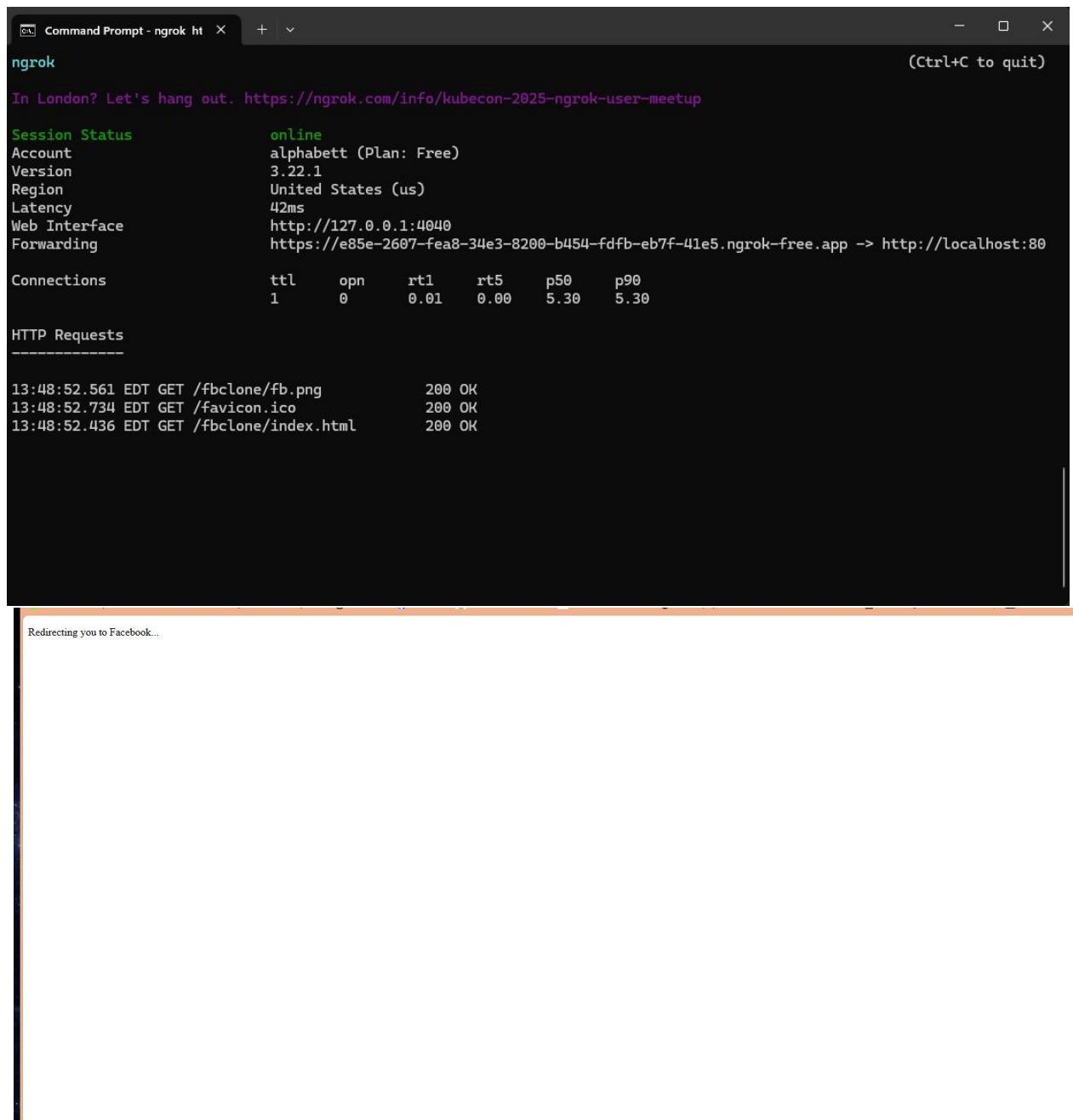
Flags:
  -h, --help      help for ngrok

Use "ngrok [command] --help" for more information about a command.

ngrok is a command line application, try typing 'ngrok.exe http 80'
at this terminal prompt to expose port 80.
C:\Users\elure\Desktop\XAMPP FILES\ngrok-v3-stable-windows-amd64>ngrok http 80
```

✓ Submit:

- Screenshot of the phishing login page -
- Screenshot of view.php showing the captured credentials
- Screenshot of redirect.html in browser
- Screenshot of your folder showing all the required files
- If using Ngrok: a screenshot of your terminal with the generated link -



The image shows a Windows Command Prompt window titled "Command Prompt - ngrok ht" with a dark background. The ngrok application is running, displaying its status and session information. Below the status, it shows a table of connections and a list of HTTP requests. The browser window below the terminal shows a message "Redirecting you to Facebook..." in a white box on a dark background.

```
ngrok (Ctrl+C to quit)
In London? Let's hang out. https://ngrok.com/info/kubecon-2025-ngrok-user-meetup

Session Status      online
Account             alphabett (Plan: Free)
Version             3.22.1
Region              United States (us)
Latency              42ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://e85e-2607-fea8-34e3-8200-b454-fdfb-eb7f-41e5.ngrok-free.app -> http://localhost:80

Connections
  ttl   opn   rt1   rt5   p50   p90
    1     0    0.01  0.00  5.30  5.30

HTTP Requests
-----
13:48:52.561 EDT GET /fbclone/fb.png          200 OK
13:48:52.734 EDT GET /favicon.ico             200 OK
13:48:52.436 EDT GET /fbclone/index.html      200 OK

Redirecting you to Facebook...
```

