✅ POC: Homographic Link Generator and Redirect Tool

◆ 1. Title

Homographic Link Generator with Redirect – A Phishing Awareness Simulation Tool

---

◆ 2. Objective

To demonstrate how attackers can use homographic (look-alike) domains combined with redirection pages to trick users into clicking suspicious links, and how such tools can be used in **security awareness training**.

◆ 3. Overview

The tool:

- Generates homographic variants of popular domains (like `youtube.com` using Cyrillic `o`)

- Creates unique redirect pages for each variant

- Deploys these pages to GitHub Pages, making them accessible via realistic phishing-style URLs

- Can be used in training or simulation environments

◆ 4. Tool Features

Feature	Description
Homograph Generation	Replaces characters with look-alike Unicode glyphs (Cyrillic, Greek, etc.)
Short Code Generator	Appends random short strings for uniqueness

HTML Redirect Template	Auto-generates redirection pages to actual URLs
GitHub Pages Deployment	Serves redirection links from GitHub
Awareness Application	Helps show users how easy it is to fall for phishing

---

◆ 5. Folder Structure

css
CopyEdit

```
Homographic-Redirect-Tool/
├── main.py
├── homograph_generator.py
├── short_links.txt
├── templates/
│   └── redirect_template.html
├── docs/                    ← GitHub Pages folder
│   ├── youtube_com_Hd4fZ.html
│   ├── google_com_Jf9tR.html
│   └── ...
```

◆ 6. Working Example

- Generated file:
  `docs/youtube_com_Hd4fZ.html`
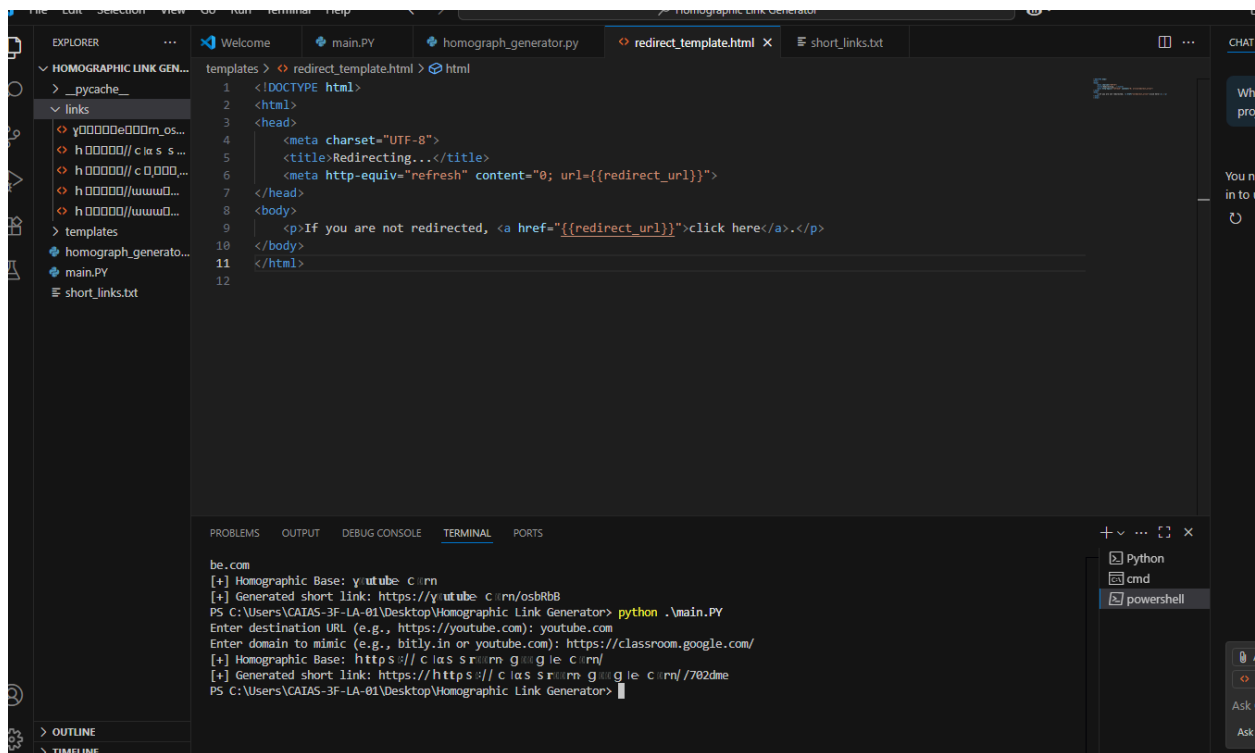
- Preview on GitHub Pages:

  `https://your-username.github.io/homograph-redirects/youtube_com_Hd4fZ.html`

- Redirection goes to:
  `https://youtube.com`

  ⚠️ Although the link looks like "youtube.com", it's actually a homograph (notice the Cyrillic 'o').

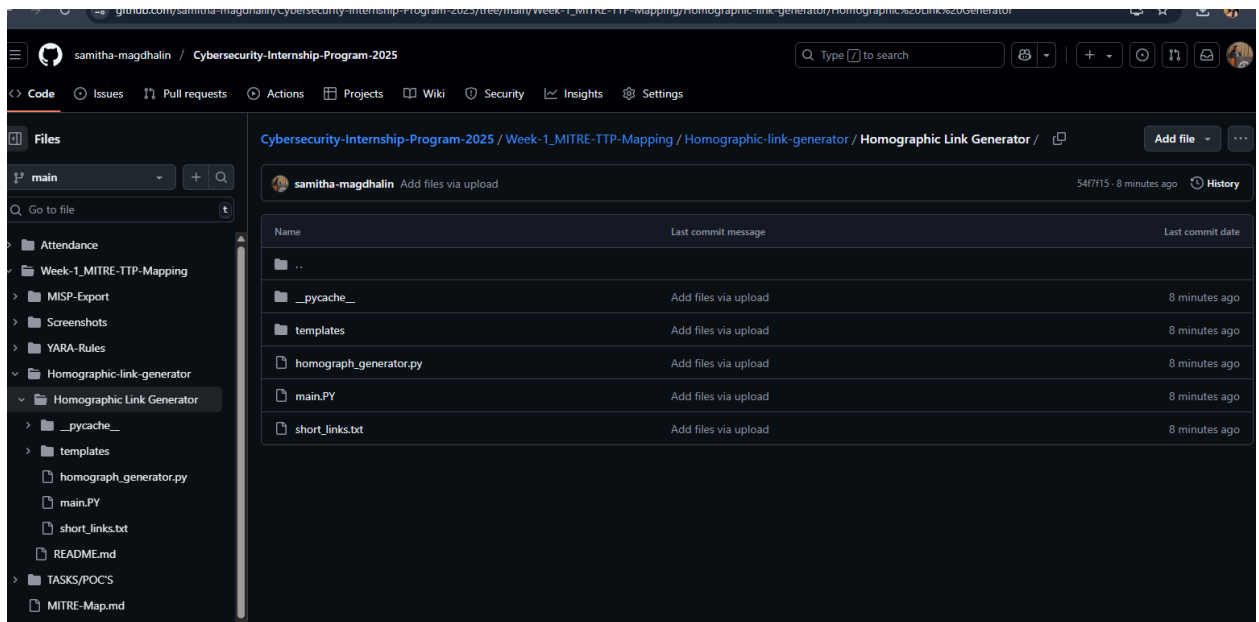# ◆ 7 . Screenshots to Include in POC Report

◆ 8. Applications & Use Case

- **Phishing Awareness Campaigns**

- **Security Workshops & Demos**

- **Internship Projects (Cybersecurity Awareness)**

- **Simulated Phishing Attack Exercises**

◆ 9. Conclusion

This project shows how easily homographic URLs and redirection tools can be created and misused. It highlights the need for better visual inspection, browser protection, and user education to stay safe online.

◆ 10. Future Enhancements

- Support for multiple domain inputs

- Real-time GUI interface

- Punycode detection and alert mechanism

- Integration with email phishing simulators