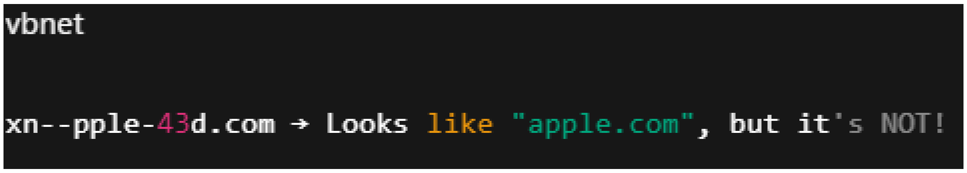
🔍 Homoglyph Domain Detector 🛡️

A Python Tool to Detect Unicode-based Homograph Links

🚨 What are Homoglyph Attacks?

Homoglyph (or **homograph**) attacks use similar-looking characters from different alphabets (like Cyrillic a vs Latin a) to create **malicious lookalike domains** that trick users into visiting phishing sites.

🧪 Example:



```
vbnet

xn--pple-43d.com → Looks like "apple.com", but it's NOT!
```

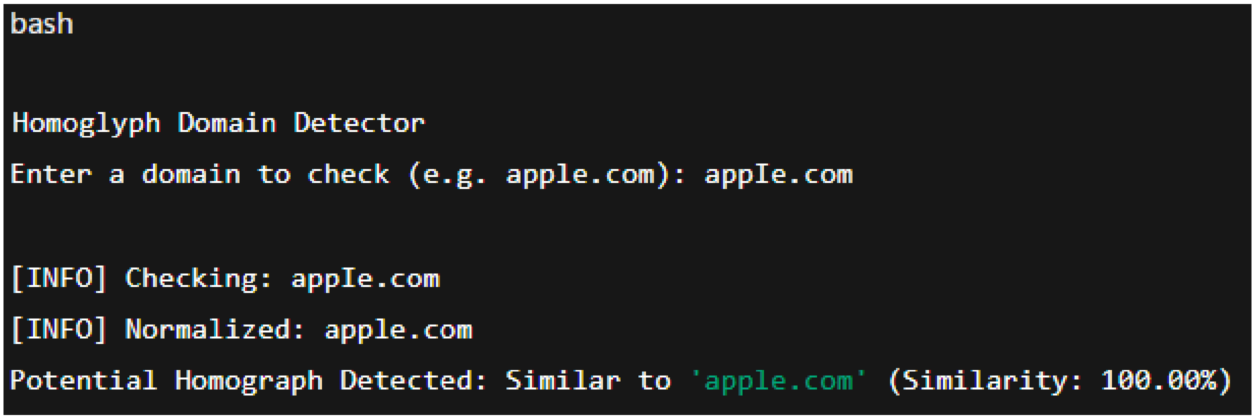
This tool detects these spoofed domains by:

- ✅ Replacing suspicious Unicode homoglyphs with standard Latin characters
- ✅ Comparing them to a trusted whitelist of domains
- ✅ Reporting anything suspicious based on similarity scores

⚙️ Key Features

- 🔤 Unicode normalization using a custom homoglyph mapping
- 🔒 Trusted domain whitelist (easily editable)
- 📏 Similarity scoring using Python’s difflib module
- 🧠 Simple CLI interface — just run and input a domain
- 💡 Great for phishing analysis and Red Team tools

🧪 Example Output



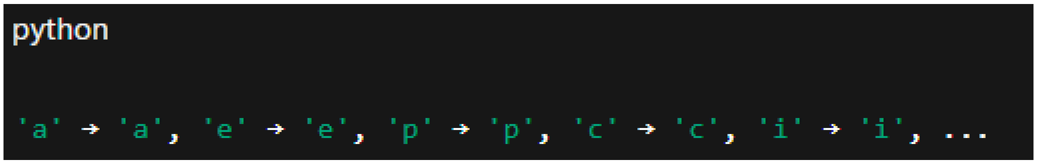
```bash
Homoglyph Domain Detector
Enter a domain to check (e.g. apple.com): appIe.com

[INFO] Checking: appIe.com
[INFO] Normalized: apple.com
Potential Homograph Detected: Similar to 'apple.com' (Similarity: 100.00%)
```

🔍 How It Works

Step 1: Unicode Normalization

The tool maps common homoglyphs to their Latin equivalents:



```python
'a' → 'a', 'e' → 'e', 'p' → 'p', 'c' → 'c', 'i' → 'i', ...
```

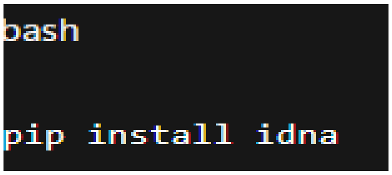
Step 2: Convert and Compare

It uses the idna library to handle IDNs and checks the normalized domain against a list of trusted domains using similarity metrics.

🧰 Requirements

- Python 3.x
- Python package: idna

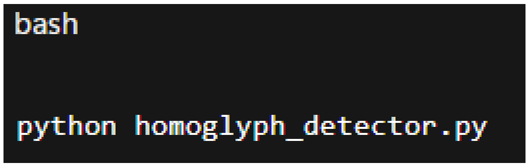
📦 Install with:



```bash
pip install idna
```

🚀 How to Use

1. Clone the repo or copy the script
2. Run the script:

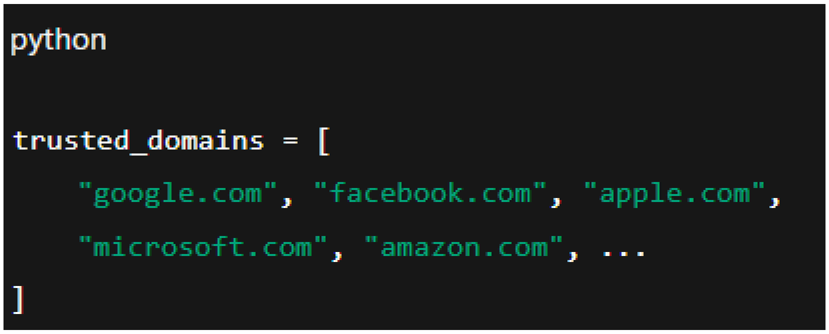


```bash
python homoglyph_detector.py
```

3. Enter a domain when prompted

🛡️ Whitelist Customization

You can easily edit the trusted_domains list in the script:



```python
trusted_domains = [
    "google.com", "facebook.com", "apple.com",
    "microsoft.com", "amazon.com", ...
]
```

✅ Legal & Ethical Use

This tool is intended **strictly for ethical and educational purposes**.
🔐 Ensure you are authorized to analyze any domain you test. Do not use it for malicious activities.

🧩 Contributing

Found a bug or want to contribute?

- 📬 Open an issue
- 🛠️ Submit a pull request

- ⭐ Star the repo if you like it!

📄 License

MIT License©

🔗 Related Tools

- 🧅 dnstwist – Domain permutation engine
- 🧬 urlscan.io – Visual analysis of URLs
- 🔍 PhishingKitHunter

⚠️ Disclaimer

This tool was developed by [VAIBHAV RATAN for ethical and educational use only. The assistance of KaliGPT was limited to organizing, formatting, and documenting the work for clarity and presentation.
This script is not intended for malicious use, and should only be executed in environments where you have explicit authorization.
The developer and contributors are not responsible for any misuse of this tool. Always ensure your actions comply with applicable laws, regulations, and ethical guidelines.