Proof Of Concept: Deceptive Link Redirection

Submitted to: Digisuraksha Parhari Foundation
By: Ankita Laxman Kolapte
Intern ID: 270

About the Tool

Description:

The Deceptive Link Redirection PoC is a Flask-based URL shortener that demonstrates how attackers can mask a malicious destination behind a legitimate-looking domain. When a user inputs a long URL, the tool generates a short code, stores it in an SQLite database, and outputs a clickable link that visually mimics a trusted site (e.g., https://google.com/abc123). However, the actual link redirects through the application to the original target, which could be a phishing page or malicious download. This PoC is intended for security testing and awareness training, highlighting the risks of open redirects and deceptive link presentation in social engineering attacks.

How It Works

1. Takes any long URL as input and generates a unique short code.

2. Stores the mapping between the short code and original URL in an SQLite database.

3. Displays a fake trusted domain (e.g., https://google.com/abc123) while the actual link points to the Flask app.

4. Redirects users to the original (possibly malicious) URL when the short link is clicked.

5. Demonstrates URL masking and open redirect risks for phishing and social engineering awareness.

Why This Tool Is Useful

1. Security Awareness Training – Helps demonstrate to non-technical users how links can be disguised to look like trusted domains.

2. Red Team Exercises – Can be used in penetration testing to simulate phishing or social engineering attacks.

3. Open Redirect Testing – Shows the risks of unvalidated redirects and how they can be exploited.

4. Educational Demonstrations – Useful for teaching students or teams about link spoofing and deceptive practices.

5. Incident Response Preparation – Helps organizations recognize suspicious links before users click them.

Use case Examples

1. Phishing Awareness Training:

- ✓ Create a short link that looks like it belongs to a trusted domain.
- ✓ Send it to employees as part of a security awareness drill.
- ✓ Measure how many users click it and provide instant training feedback.

2. Red Team Social Engineering Test:

- ✓ Use the tool during a penetration test to simulate how attackers disguise malicious links.
- ✓ Redirect to a controlled environment that logs user actions without real harm.

3. Educational Cybersecurity Workshop:

- ✓ Demonstrate to students how URL masking works in real-time.
- ✓ Show them the difference between the visible text of a link and its actual destination.
- ✓ Teach how to inspect links before clicking.

Who Should Use It

This POC is primarily for:

- **1. Raise Security Awareness** : Helps users and teams understand how legitimate-looking links can hide malicious destinations.
- **2. Simulate Real Attacks Safely** : Allows security teams to replicate phishing-style redirections without exposing users to actual threats.
- **3. Test User Vigilance** : Measures how well employees verify URLs before clicking, improving organization-wide security posture.
- **4. Support Training & Education** : Provides a hands-on demonstration for workshops, awareness campaigns, and cybersecurity classes.
- **5. Highlight Open Redirect Risks** : Shows how unvalidated redirects can be exploited for phishing, malware distribution, and social engineering.

Future Enhancements:

1. Click Tracking & Analytics : Log the number of times each short link is clicked, along with IP, browser, and timestamp.

2. Custom Short Codes : Allow the user to choose a custom short code instead of random generation.

3. Password-Protected Links : Require a password before redirecting to the original URL for controlled testing.

4. Link Expiry Feature : Set expiration dates for short links to limit the window of exposure.

5. Phishing Simulation Mode : Integrate with training platforms to show a warning or training page after redirection.

6. Enhanced Fake Domain Customization : Allow users to choose from multiple trusted-looking fake domains for more realistic simulations.

7. Admin Dashboard : Provide a web interface for managing, editing, and deleting shortened links.

AI Integration Possibility:

1. Malicious URL Detection : Integrate an AI model to scan submitted URLs and predict whether they are phishing, malware, or safe before shortening.
2. User Behavior Analysis : Use AI to track and analyze click patterns to identify which users are more susceptible to deceptive links.
3. Smart Domain Suggestions : AI could suggest the most convincing fake domains for a phishing simulation based on target context.
4. Automated Phishing Templates : Generate realistic but safe phishing landing pages for training exercises.
5. Threat Intelligence Integration : AI could cross-check submitted URLs with known threat databases to classify risk levels automatically.
6. Adaptive Difficulty for Training : AI could adjust the realism of the fake links based on how well users perform in security awareness drills.