Information Security Proposal

The Two-Factor (2FA) Bypass Proxy

Attack Focus: Real-time Session Hijacking and 2FA Evasion.

Submitted by:

Name	Roll Number
Asim Khan Niazi	22F-8773
Qasim Naveed	22F-3298
Zahid Khalil	22F-3573

Course / Instructor:

Information Security / Dr. Umar Aftab

Date: 11/19/2025

Department of Computer Science
National University of Computer and Emerging Science
Chiniot Faisalabad, Pakistan
2025

Project Proposal

Project Title: The Two-Factor (2FA) Bypass Proxy

Focus: Real-time Session Hijacking and 2FA Evasion

Overview:

This project involves developing a highly sophisticated Man-in-the-Middle (MITM) reverse proxy using frameworks such as Flask or Django, integrated with libraries like httpx for live traffic relay. The proxy operates in real-time, capturing user credentials, 2FA codes, and authenticated session tokens.

Additionally, this project includes performing phishing attacks as part of the testing methodology. A phishing page is created to lure victims into entering their login credentials and 2FA codes. The phishing component works alongside the MITM reverse proxy to simulate realistic attack scenarios and demonstrate how modern phishing campaigns can combine cloned interfaces with real-time relayed content to bypass security mechanisms.

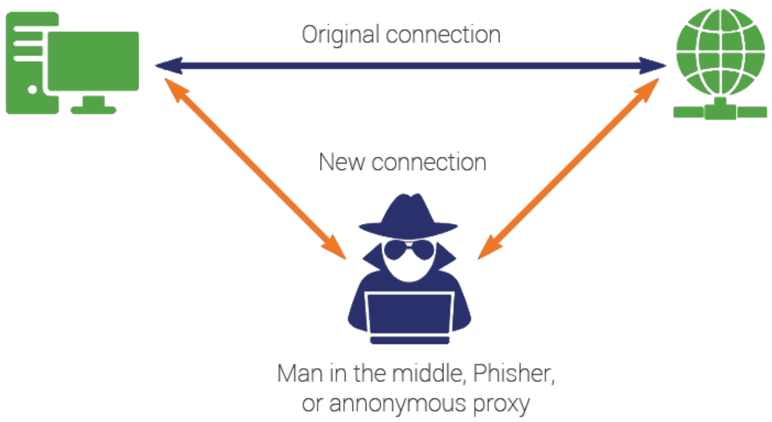

Figure 1 Man-in-the-Middle (MITM) Attack Diagram

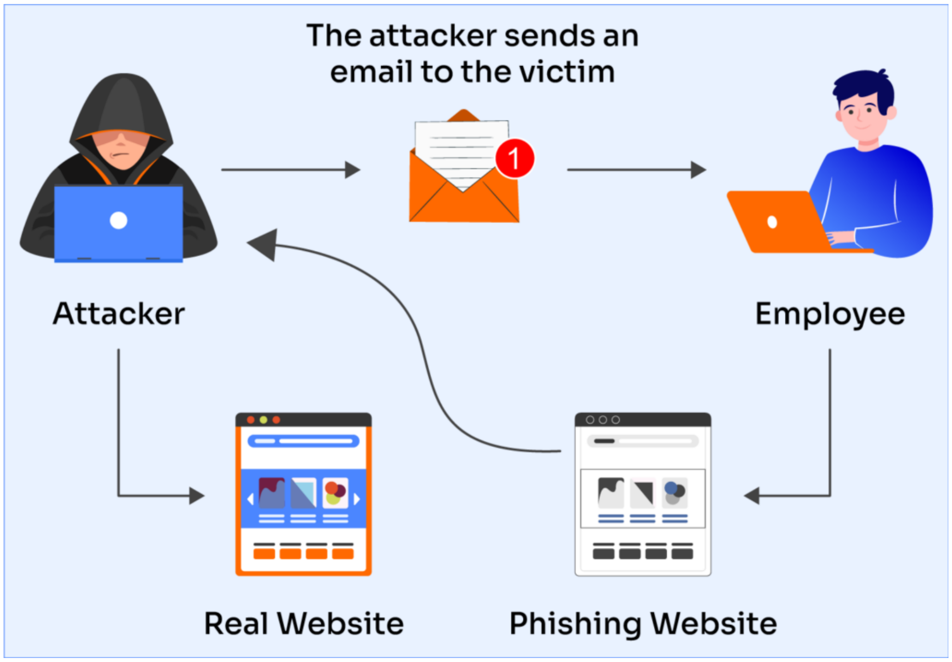

Figure 2 Step-by-Step Flow of a Standard Phishing Attack

Key Functionalities:

1. Real-time Relay

The proxy acts as a live intermediary between the victim and the legitimate website. Unlike simple phishing pages, it relays traffic in real time, making the interaction seamless.

2. 2FA Capture

When the legitimate site prompts the user for their Time-based One-Time Password (TOTP) or SMS code, the proxy captures this code during the POST submission. The system then instantly forwards this code to the legitimate website before expiration.

3. Session Token Theft

After successful authentication, the real server issues an authenticated session cookie/token. The proxy intercepts this token and logs it, allowing persistent account access without needing credentials or 2FA again.

Why This Attack is Dangerous:

This method, often known as session token hijacking or token grabbing, effectively bypasses standard 2FA protection. Since authentication occurs on the attacker's proxy, the attacker gains full privilege access without needing to break or guess any 2FA mechanism.

Mechanism Summary:

- The victim enters credentials on a proxied login page controlled by the attacker.
- The attacker forwards the credentials to the real server.
- The server requests a 2FA code; the attacker relays the prompt.

- The victim enters the 2FA code into the attacker's fake page.
- The attacker captures and forwards the code instantly.
- The real server authenticates, sending back a session cookie.
- The attacker logs the cookie and seamlessly displays the final page to the victim.

This project demonstrates advanced weaknesses in 2FA systems when combined with MITM techniques and emphasizes the importance of phishing-resistant authentication methods such as FIDO2/WebAuthn.