# Abstract

Phishing remains a prevalent threat in cybersecurity, often targeting unsuspecting users through deceptive means to extract sensitive information. This project focuses on leveraging Kali Linux, a popular penetration testing platform, to investigate phishing techniques using Zphisher, an advanced phishing tool. Zphisher automates the creation of phishing pages and provides various attack vectors, making it a potent tool for simulating phishing attacks.

The primary objective of this project is to demonstrate the capabilities of Zphisher in conducting phishing attacks and to analyze its effectiveness in a controlled environment. Through a series of experiments, we will create and deploy phishing pages that mimic popular services and evaluate their potential to deceive users. The project will also involve assessing the security measures that can mitigate such eattacks and proposing best practices for enhancing user awareness and system defenses.

By simulating real-world phishing scenarios, this project aims to highlight the vulnerabilities inherent in current cybersecurity practices and provide insights into improving protection strategies against phishing threats. The findings will contribute to a deeper understanding of phishing techniques and the development of more robust security protocols to safeguard sensitive information.