Automating Website Information Gathering for Penetration Testing Using Bash Scripting

Abstract:

In penetration testing, information gathering is a critical phase that involves collecting and analysing data from various sources, including websites. However, the manual process of website data collection and analysis can be time-consuming and error-prone, leading many testers to adopt website information gathering automation tools. This project aims to develop a tool using bash scripting that integrates existing tools available in the market, such as Nmap, Dirb, and Ping, to automate the process of website data collection and analysis. The tool will leverage web scraping, web crawling, and parsing techniques to gather information on website content, structure, and performance, providing valuable insights to inform decision-making in penetration testing. By automating the information gathering phase, the tool will save time and resources while improving the accuracy and speed of data analysis. The project will demonstrate the potential of website information gathering automation to enhance the effectiveness of penetration testing and improve the security of organizations in any industry.