Technology Stack:

In our project, we explored a variety of cybersecurity tools to analyze and address potential threats, offering solutions for the evolving digital landscape:

1. **Web Technologies**:
    - **HTML, CSS, JavaScript** – These front-end technologies were used to evaluate web application vulnerabilities such as Cross-Site Scripting (XSS) and other common security misconfigurations.
    - **PHP & MySQL** – A popular backend stack commonly found in vulnerable applications like bWAPP, which allowed us to test for issues like SQL Injection (SQLi).
    - **Node.js & Express** – With modern web applications increasingly relying on Node.js, this stack became essential for testing security flaws in APIs and authentication processes.
2. **Penetration Testing Tools**:
    - **Burp Suite** – A key tool for intercepting and modifying HTTP requests, helping us test for authentication weaknesses, SQL Injection, and Cross-Site Scripting (XSS).
    - **OWASP ZAP** – A powerful open-source security scanner used to detect common vulnerabilities, including broken authentication and improper security configurations.
    - **SQLMap** – A robust tool designed to automate the detection of SQL injection vulnerabilities and test for potential data exfiltration risks.
    - **Nikto** – A web server scanner utilized to identify outdated components, misconfigurations, and common vulnerabilities that could lead to exploitation.
    - **Hydra** – A highly effective brute-force tool for testing login forms and network services for potential weaknesses in authentication.
3. **Vulnerable Testing Platforms**:
    - **bWAPP (Buggy Web Application)** – A deliberately insecure web app used to practice simulating real-world attacks, including SQLi, XSS, IDOR, and flawed authentication mechanisms.
    - **OWASP Juice Shop** – A modern application designed to provide a safe environment for testing vulnerabilities from the OWASP Top 10, enabling us to identify weaknesses in real-world scenarios.

- **DVWA (Damn Vulnerable Web App)** – Another platform used for testing web application security weaknesses, allowing for the exploration of common vulnerabilities in a controlled and legal setting.