**Technology Stack :**

**In this project, we explored various cybersecurity tools to understand threats and solutions in the digital age:**

**1. Web Technologies :**

These technologies help analyze web application vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection (SQLi), and Security Misconfigurations.

* HTML, CSS, JavaScript – Used for creating and testing front-end vulnerabilities like XSS and client-side security flaws.
* Django & Flask (Python) – Web frameworks where security measures like CSRF protection, authentication mechanisms, and session management can be tested.
* MongoDB & PostgreSQL – Used to explore NoSQL Injection and database security misconfigurations.

**2. Penetration Testing Tools :**

* Nikto – A web server scanner to check for misconfigurations, outdated components, and common exploits.
* NoSQLMap – A tool for testing NoSQL Injection attacks on MongoDB, CouchDB, and other NoSQL databases.
* John the Ripper – A password-cracking tool for testing password security and hash vulnerabilities.
* Wireshark – A network traffic analysis tool to detect suspicious activities, packet sniffing, and MITM attacks.
* Postman – Used for API penetration testing and authentication testing.

**3. Vulnerable Testing Environments :**

* DVWA (Damn Vulnerable Web App) – Another platform used to test web security weaknesses in a controlled setting.
* Metasploitable 2/3 – A virtual machine designed to test network and system security vulnerabilities.
* VulnHub – Provides virtual machines with different security challenges for ethical hacking practice.