Cyber Sentinel - A vulnerable application

Team: Devanssh Agarwal (2010110220), Snehasri Ravishankar (2010110638), Suchit Reddi (2010110507).

Malware is malicious software including but not limited to spyware, ransomware, viruses, and worms. Once inside a system, malware can:
- Block access to critical components of a network and render systems inoperable
- Install additional harmful software
- Discretely derive information by transmitting data from the hard drive (spyware)

Cyberattacks are unwelcome attempts to steal, expose, alter, hijack, or destroy data through unauthorized access to computer systems. These days, most website or application **developers are unaware** of the different vulnerabilities in their programs.

The main aim of our project is to **create awareness of common vulnerabilities** by creating a vulnerable application that simulates different types of cyberattacks and then shows how to mitigate them. We focus primarily on web application vulnerabilities as they are less complex but more common, increasing their damaging capacity.

After demonstrating how these attacks are carried out, we show how to **patch a website against the demonstrated attack**. We will implement thorough front-end visual aids to better understand these attack processes and their step-by-step patching.

We will have code segments illustrating the security flaws and how to patch them, using languages and frameworks including but not limited to PHP, HTML, and CSS. We will secure the vulnerable web application by containerizing it with docker, which is like a virtual machine.

Example of an attack: A Structured Query Language (SQL) injection occurs when an attacker forces a server using SQL to reveal information it usually would not. This could happen just by submitting malicious code into one vulnerable search box. This attack can be prevented by methods like input validation, and not taking direct user input without sanitization.