Cyber Sentinel – An intentionally “vulnerable” web application

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 yet dangerous vulnerabilities by creating a vulnerable web 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 **tutorials** to better understand these attack processes, vulnerable code, and its 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: Cross-Site Scripting (XSS) attacks are done by injecting scripts into trusted websites. Malicious code leading to stolen cookies/session tokens can be sent to different end users in the form of browser side scripts using this vulnerability. This vulnerability can be patched by not allowing the insertion of <script> tag, generating Anti-CSRF tokens, or fixing the input that can be given.