**Week 1:**

The assessment reveals the absence of SQL injection vulnerabilities and the security concern that passwords are stored within the database.

**Vulnerabilities identified include:**

1. The admin page is accessible without requiring authentication.

2. Unauthorized individuals with technical knowledge can access the admin page by navigating to localhost3000/admin, thereby gaining administrative privileges.

3. Cross-site scripting (XSS) vulnerabilities are present on the signup form.

**Recommendations for improvement are as follows:**

1. Implement a login page prior to granting access to the admin profile to enhance security.

**Additional observations include:**

- The server discloses version information through the "Server" HTTP response header, posing a low risk, as it may aid attackers in identifying potential vulnerabilities.

- The absence of the X-Content-Type-Options header, which is recommended to be set to 'nosniff'. This omission permits older browsers, such as certain versions of Internet Explorer and Chrome, to perform MIME-sniffing on responses, potentially leading to misinterpretation of the content type. Modern browsers, including the latest versions of Firefox, rely on the declared content type, thereby mitigating this risk.MIME-sniffing.