I have seen website which are designed to illustrate common security challenges, you encounter various issues that can pose potential threats to user data and system integrity.

1. **Secure Coding Practices**
Problem:
In order to ensure that the application does not contain poor coding, it is important to implement best practices and regularly conduct code reviews. This will help to identify and address any potential coding issues or vulnerabilities, thus improving the overall quality and security of the application.
Solution:
In order to ensure that the application does not contain poor coding, it is important to implement best practices and regularly conduct code reviews. This will help to identify and address any potential coding issues or vulnerabilities, thus improving the overall quality and security of the application.

2. **Session Management**
Problem: If the session is not managed properly, it could potentially result in hacking and unauthorized access, creating vulnerabilities that expose sensitive information and compromise the security of the system. Inadequate session management opens the door for malicious individuals to exploit weaknesses, gaining illicit entry to confidential data and potentially causing irreparable damage to the network or infrastructure.

Solution: If the session was already active before login, it should automatically log out and initiate a new session through login. Additionally, the logout process should be completed in its entirety, ensuring a smooth transition between sessions.

3. **Input Validation**
Problem: The absence of bounds checking allows attackers to overwrite adjacent memory regions, leading to buffer overflow vulnerabilities.
Solution:
To improve data security, it is important to implement strict bounds checking for all input data. This means implementing measures to ensure that the data being written to buffers does not exceed their allocated size. By closely monitoring the sizes of input data and setting clear limits, we can prevent buffer overflows and potential vulnerabilities in our system.

4. **Authentications and password management**
Problem: To effectively protect sensitive information and personal data from unauthorized access and potential security breaches, it is crucial to implement robust security measures, such as encryption protocols, multifactor authentication, regular vulnerability assessments, and continuous monitoring of network activities.
Solution: To ensure the utmost security, it is essential to adopt a secure and reliable system for storing all passwords. This system should incorporate advanced encryption and decryption methods to safeguard sensitive information. Moreover, it should enforce a password policy that includes requiring passwords to be a minimum of eight characters and include a combination of words and letters. Additionally, it is advisable to promote regular password updates, such as requiring users to change their passwords every six months. By

implementing these measures, users can have confidence in the safety and integrity of their stored passwords.

5.**Output Encoding** :
Problem: In order to achieve a successful and effective encoding process, it is essential to implement the necessary steps and techniques.
Solution: We should ensure that all encoding tasks are conducted exclusively on a trusted system. It is crucial that we prioritize the use of a secure environment for encoding purposes.