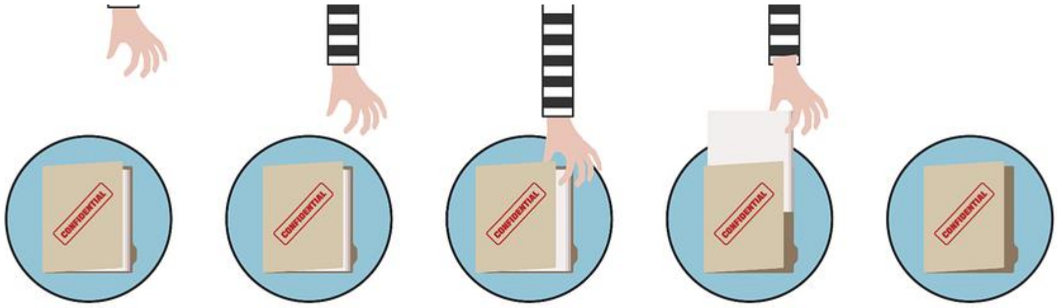
Task 16 : 7. Identification and Authentication Failures



Authentication and session management constitute core components of modern web applications. Authentication allows users to gain access to web applications by verifying their identities. The most common form of authentication is using a username and password mechanism. A user would enter these credentials, and the server would verify them. The server would then provide the users' browser with a session cookie if they are correct. A session cookie is needed because web servers use HTTP(S) to communicate, which is stateless. Attaching session cookies means the server will know who is sending what data. The server can then keep track of users' actions.

If an attacker is able to find flaws in an authentication mechanism, they might successfully gain access to other users' accounts. This would allow the attacker to access sensitive data (depending on the purpose of the application). Some common flaws in authentication mechanisms include the following:

- **Brute force attacks:** If a web application uses usernames and passwords, an attacker can try to launch brute force attacks that allow them to guess the username and passwords using multiple authentication attempts.
- **Use of weak credentials:** Web applications should set strong password policies. If applications allow users to set passwords such as "password1" or common passwords, an attacker can easily guess them and access user accounts.
- **Weak Session Cookies:** Session cookies are how the server keeps track of users. If session cookies contain predictable values, attackers can set their own session cookies and access users' accounts.

There can be various mitigation for broken authentication mechanisms depending on the exact flaw:

- To avoid password-guessing attacks, ensure the application enforces a strong password policy.
- To avoid brute force attacks, ensure that the application enforces an automatic lockout after a certain number of attempts. This would prevent an attacker from launching more brute-force attacks.
- Implement Multi-Factor Authentication. If a user has multiple authentication methods, for example, using a username and password and receiving a code on their mobile device, it would be difficult for an attacker to get both the password and the code to access the account.

Answer the questions below :

1. I've understood broken authentication mechanisms.
A. No answer needed