Task 5 : 2. Cryptographic Failures

Cryptographic Failures

A **cryptographic failure** refers to any vulnerability arising from the misuse (or lack of use) of cryptographic algorithms for protecting sensitive information. Web applications require cryptography to provide confidentiality for their users at many levels.

Take, for example, a secure email application:

- When you are accessing your email account using your browser, you want to be sure that the communications between you and the server are encrypted. That way, any eavesdropper trying to capture your network packets won't be able to recover the content of your email addresses. When we encrypt the network traffic between the client and server, we usually refer to this as **encrypting data in transit**.
- Since your emails are stored in some server managed by your provider, it is also desirable that the email provider can't read their client's emails. To this end, your emails might also be encrypted when stored on the servers. This is referred to as **encrypting data at rest**.

Cryptographic failures often end up in web apps accidentally divulging sensitive data. This is often data directly linked to customers (e.g. names, dates of birth, financial information), but it could also be more technical information, such as usernames and passwords.

At more complex levels, taking advantage of some cryptographic failures often involves techniques such as "Man in The Middle Attacks", whereby the attacker would force user connections through a device they control. Then, they would take advantage of weak encryption on any transmitted data to access the intercepted information (if the data is even encrypted in the first place). Of course, many examples are much simpler, and vulnerabilities can be found in web apps that can be exploited without advanced networking knowledge.

Indeed, in some cases, the sensitive data can be found directly on the web server itself.

The web application in this box contains one such vulnerability. To continue, read through the supporting material in the following tasks.

Answer the questions below :

1. Read the introduction to Cryptographic Failures and deploy the machine.
A. No answer needed