A6- Sensitive data exposure

What is sensitive data?

Banking information (account number, credit card numbers, transactions)

Health information

Personal information (date of Birth, SSN/SIN)

Social security questions and answers

User account/passwords

When?

When the sensitive data (the data which needs more protect is exposure)

What can be done?

Financial loss

Identity hi-jacking

Decreased brand trust

When can happen ?

During the transport of data from client to server and server to client

At database

When displayed in the application

How to prevent?

Encrypt the data during the transport layer and the application layer(Use https transport, use up to date certificate, encrypt sensitive data at database and file systems, ensure passwords are stored as encrypts using password protection scheme, )

Minimize the data surface area(only store the sensitive data when necessary, only transport/show sensitive data when needed)

Use the latest encryption algorithms

Disable auto complete on forms that collect data

Disable caching on forms that collect data