A6 Sensitive Data Exposure

Mika Salmela

What Is Sensitive Data Exposure?

IT systems usually save in a database user's personal information such as passwords, credit card numbers, house address', telephone number, id number etc.

When the system is not protected effectively from unauthorised access there is a high probability that a hacker might exploit that vulnerability and steal that information. That vulnerability is "Sensitive Data Exposure".

Am I Vulnerable to Data Exposure?

- The first thing you have to determine is which data is sensitive enough to require extra protection.
- For all such data, ensure:
  - It is encrypted everywhere it is stored long term, including backups of this data.
  - It is encrypted in transit, ideally internally as well as externally. All internet traffic should be encrypted.
  - Strong encryption algorithms are used for all crypto
  - Strong crypto keys are generated, and proper key management is in place, including key rotation.
  - Proper browser directives and headers are set to protect sensitive data provided by or sent to the browser.

Examples Attack Scenarios

- An application encrypts credit card numbers in a database using automatic database encryption. This means also decrypts this data automatically in some point. This allowing an SQL injection flaw to retrieve credit cardnumbers in clear text. Attacker then replays this cookieand hijacks the user's session, accessing all their private data.
- A site simply doesn't use SSL for all authenticated pages. So you can simply monitors network traffic, and steals the user's session cookie. So then you can replays this cookie and hijacks the user'ssession, accessing all their private data.
- "The password database uses unsalted hashes to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password file. All the unsalted hashes can be exposed with a rainbow table of precalculated hashes." ?!!?!?