**Sensitive Data Exposure**

1 min

Sensitive data exposure is when sensitive data is not protected correctly. It includes everything from password hashes to health records to financial information.

There is some overlap between this and authentication failures, and many cryptography-based ways that authentication can go wrong also belong to this category.

Sensitive data exposure is bad for the people whose data is being exposed and the organization that failed to protect it. In addition to the loss of trust, it's a fantastic way to get in trouble with regulators, get sued, or get hit with large fines.

The best way to avoid sensitive data exposure is not to store sensitive data in the first place. If you do have to store sensitive data, it needs to be encrypted in transit and at rest, using up-to-date encryption algorithms and protocols, the use of which are adequately enforced. It would also be prudent to minimize the sensitive data you store.

Other considerations include the proper generation of keys and initialization vectors, the proper identification of sensitive data, and the use of sufficiently random number generators.