Sensitive Data Exposure

What is Sensitive Data Exposure ?
Sensitive data exposure occurs when an application, company or other entity exposes personal/company related data.

Each data we see has some importance. Either in the webpage or captured in tools like Burp.
So first thing we need to determine is which data is sensitive enough to require adequate protection.
Like session tokens, API keys, passwords location, credit card details, Personal information,and nowadays s3 bucket names,. Also Leads to path traversal.

Ex – which info is sensitive	Causes
1.Banking Info – Credit card number, PIN, ph number	Financial Loss
2.Health Info – PII, Health Company	Identity HiJack
3.Personal Info – DOB, ph numb	Social Engineering
4.Web Dev Info – Version built on	Ease to break into website*

What OWASP says?
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Infomation Disclosure

Major Sources
1.Reveiling names of hidden directory(tools -dirb) like robots.txt , .bak files, .htaccess, .backup, /admin .sql
2.Explosing database table or column names in error messages
3.Unnecessary exposing of high sensitive info such as credit card or even a phone .
4. Git hub repo – Cloud access key ID and secret access key , Tool – prowler,Scout suit,

Data at rest and transit?

Data at Rest – local storage, pendrive ..
Data at Transit – Data which moves from one location to another via internet.
Both are at risk , but when at Transit, We need to ensure that it is encrypted well with HTTPS, SSL, TLS.
Why this encryption here – Credit card transaction if there is a MIM attack, we need to ensure the details are encrypted well not in a readable format.

Juice Shop – Labs
Portswigger Labs

Remediations

1. Ensure strip the developer comments

2.Use Simple error messages, not provide any clue to attacker about application is build
3.Ensure everyone involved in the development of website is aware of what data is being exposed. Ex- if a server version is visible, it doesnt matter to the db guy who is unaware of consequences.
4.Disable auto-complete forms as much as possible which has sensitive data, we can see this implemented in passport portal.

Possible Questions??

1. Mitigation
2. Encryption
3. Recon