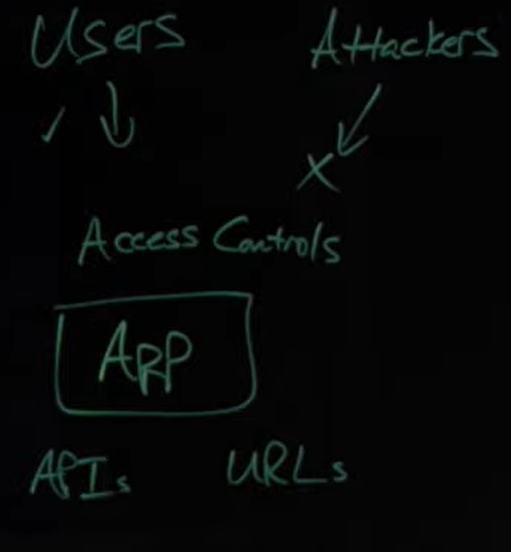
OWASP TOP 10:

1.Broken Access Control:



Prevention:

1.Denial by default.

2.Access control Mechanism and Monitoring.

3.Log Access Control failures.

4.Restriction of Access Outside the Org. premises.

**2.Cryptographic failures:**

1.Implemantation of weak/compromised algorithms.

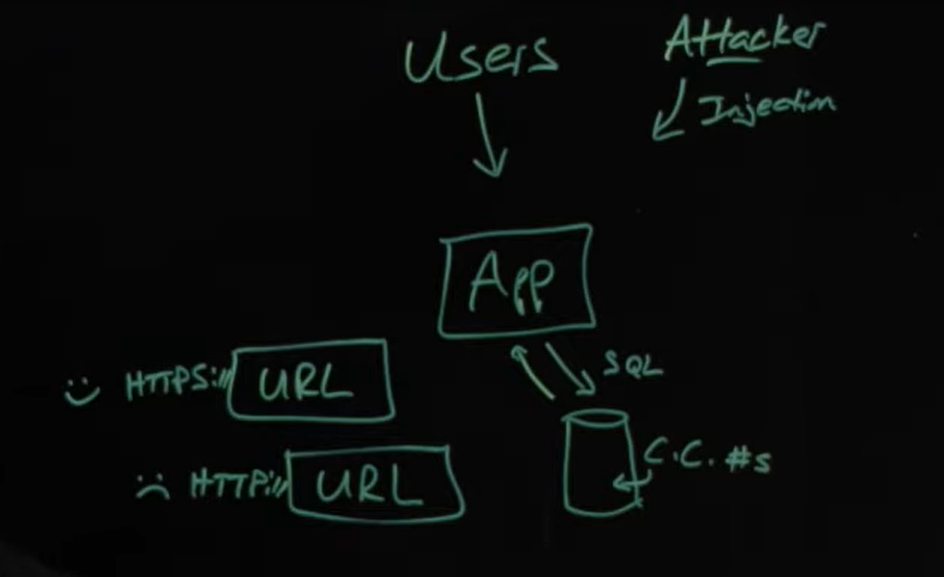
2.Cryptographic focus on security of data in transit/rest.

Open-source: Google Tink, Libsodium.

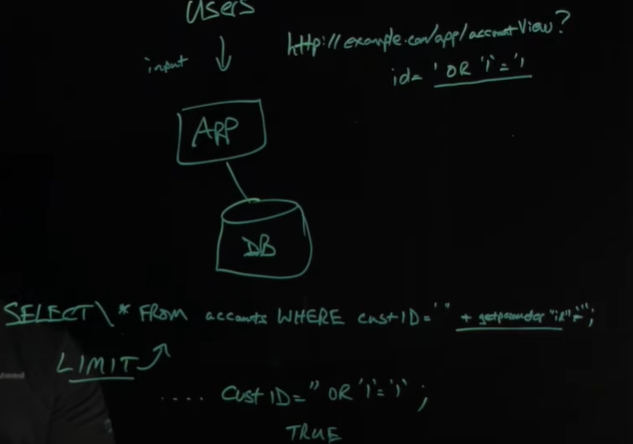
Ex: Sensitive Data, Passwords, Credit Cards, Personal Data, Health Information.

Privacy laws: GDPR

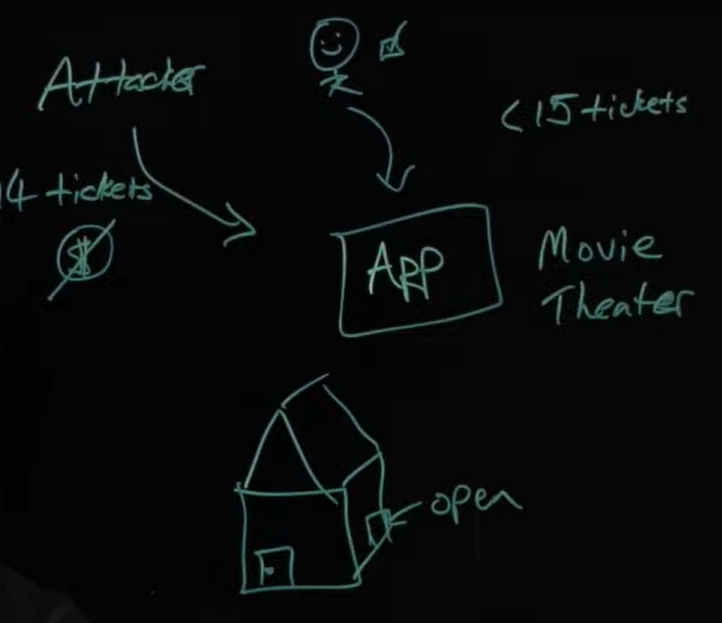
Regulations: PCI Data Security Standards (PCI DSS)



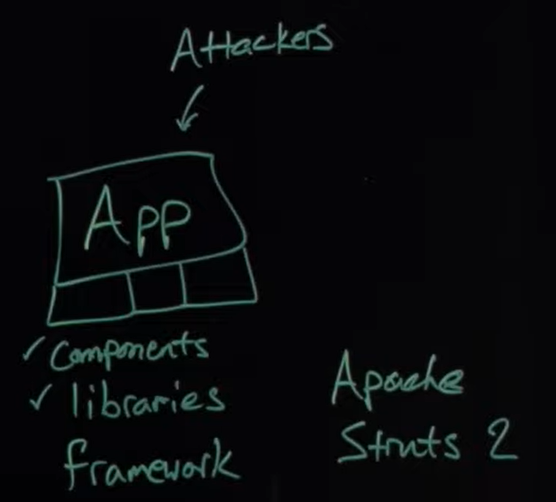
**3.Injection:**

****

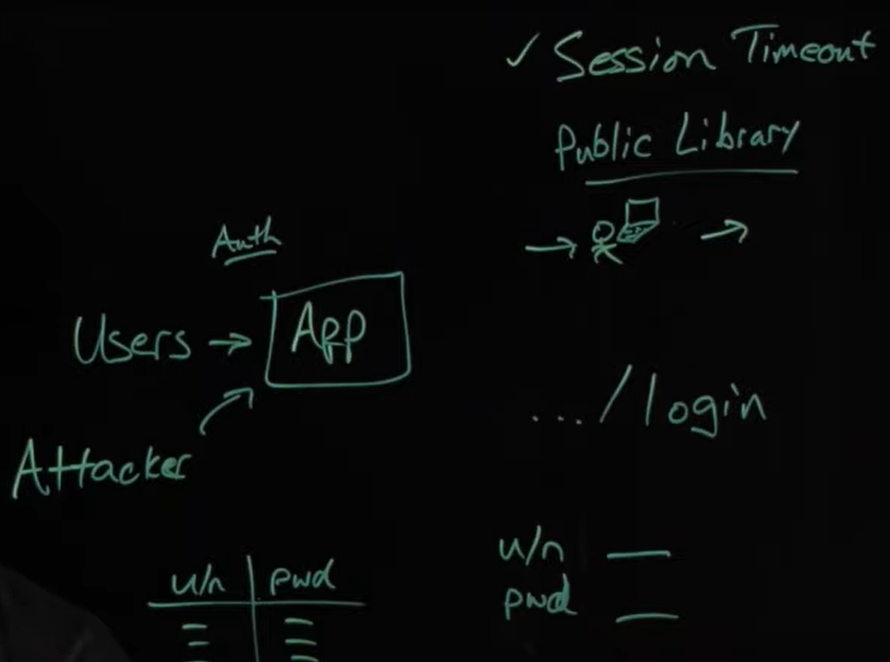
**4.Insecure Design:**

****

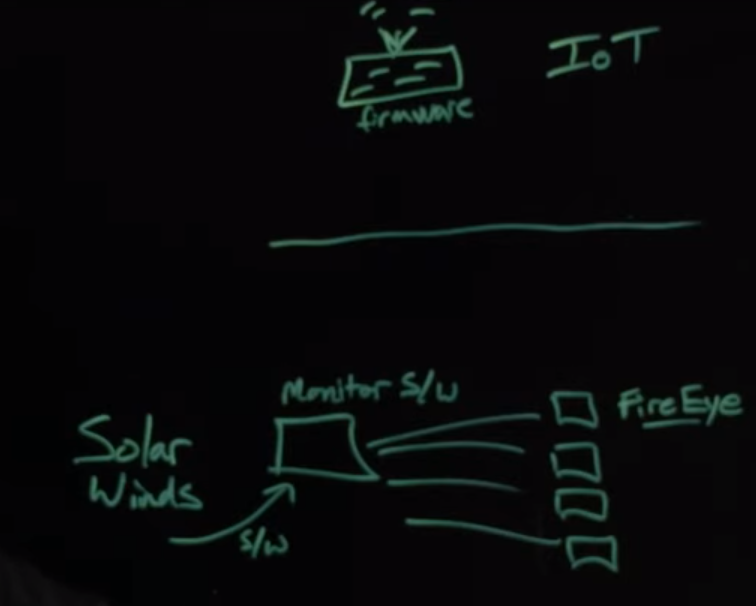
**5. Security Misconfiguration:**

****

**6.Authentication and Identification:**

****

**7.Software and Data Integrity:**

****

**9. Security Logging and Monitoring:**

**10.Serveer Side Request Forgery.**