**Stride Model**

|  |  |
| --- | --- |
| Spoofing | * Monitoring unencrypted user credentials on network * Phishing attacker can catch user credentials and spoof its identity * SQL injection could cause the same if not handled properly * Stored XXS causing to send credentials to attacker each time its typed * If DB is attack or leaked and credentials are not enctypted+salted then it would cause identity theft * If password is not hashed+salted could be vulnerable to dictionary attacks * Also if password is not complicated enough it could be broken quite easily with brute force * Lack of logic of password typing retries |
| temper | * Stored XXS means tempering with DB data for good and can cause various kinds of damage * Altering password of users stored in DB or in traffic |
| repudability | * One can delete data from DB with no records of who did it * One can add users to DB with no premission check * If there are permissions and one of them was changed you can’t decide who cause this * Attacker can store XSS with no traces except for the data which was stored |
| Information disclosure | * SQL injection can cause data leakage of details and passwords of users * The structure of DB can disclose data about the users and website * XXS can disclose to attacker about each new user who is register to the website * Also in phishing attack |
| DOS | * Brute force network attacks method without any defense mechanism would cause sirious DOS * Deletion of partial\all of DB would leave users unserviced * Altering passwords or email tempering with details would leave certain users unable to use the system |
| Eleavation of privilege | * Password theft of users will grant them unauthorized access to info and to alter data * Unencrypted password would ease on attacking and cracking it * SQL injection can reveal data which attacker shouldn’t know |