**Part C – Stride Model**

|  |  |  |
| --- | --- | --- |
| # | Weakness point description | Relevant Threat |
| 1 | Sql commands are not using parameters. | Spoofing Identity:  Connecting to other users without knowing their passwords.  Tampering with Data:  Changing clients and users’ information.  Information Disclosure:  Presenting all the clients in the system.  Elevation of Privilege:  Gaining admins’ privileges without having a user account. |
| 2 | User input is not encoded. | Information Disclosure: Exposing sensitive data from database tables. |
| 3 | Email credentials stored unencrypted in database. | Denial of Service:  Disabling the email service, thereby preventing users from utilizing the "forgot password" feature. |
| 4 | Salt value stored in database unencrypted. | Spoofing Identity:  Cracking users’ passwords is easier. |
| 5 | Adding clients without knowing which user added them. | Repudiation:  Users can attempt abnormal actions without being tracked or detected.  Denial of Service:  Attackers can flood the system with an overwhelming number of clients, causing the database to crash or consume all available memory capacity. |
| 6 | Sign in without multifactor authentication. | Spoofing Identity:  Signing into other users without their permission and knowing. |
| 7 | Data stored in one place. | Denial of Service:  Deletion of even a single table could lead to a complete shutdown of the website, resulting in permanent data loss. |
| 8 | Db exposed to anyone with the DbConfig.json file. | Tampering with Data:  Changing the tables in the database.  Repudiation:  Changing data manually without being tracked.  Information Disclosure:  Unauthorized access to sensitive unencrypted data.  Elevation of Privilege:  Gaining complete database access and control. |
| 9 | System screen does not check whether user is logged in or not. | Elevation of Privilege:  Gaining users’ privilege without logging in. |
| 10 | Using third party libraries without checking them for vulnerabilities. | Elevation of Privilege:  Gaining unauthorized access to sensitive functionality or data within the system. |
| 11 | Clients’ information stored unencrypted. | Information Disclosure:  Exposing sensitive client’s information to everyone. |
| 12 | Application users may perform malicious DB manipulations as system is using administrative access DB user. | Denial of Service:  Deleting database or tables could lead to website functionality shut down.  Tampering with Data:  Modifying data without permission. |