STRIDE MODEL

|  |  |  |
| --- | --- | --- |
|  | Weakness point Description | Relevant thread |
| 1 | user register | **Information Disclosure**  When the system is not protected, a person who registers in the system (that is, enters certain information into the system such as personal details) which are not encrypted and can get potentially to Eve. |
| 2 | Adding a customer to the system | **Elevation of privilege**  There is no difference in the permission between a regular user and the admin, everyone that uses the system has access to the customers of the company, and can add fake customer. |
| 3 | Login | **Tampering with data**  Eve can enter some kind of query or cause other damage and thus disrupt the system (such as deleting a table or making any changes in the DB)  **Spoofing**  There is no two-step verification when entering our system (for example, verification through an additional means such as phone or email), which means that a person who accidentally discovered the username and password of another person can enter the system and impersonate that person. |
| 4 | Sensitive data is stored in configuration file unencrypted | **Tampering with data**  Changing configuration files  **Information Disclosure**  Unauthorized access to unencrypted data in sensitive configuration files. |
| 5 | 3 login attempted | **Spoofing**  If someone is trying to impersonate someone else, he can try unlimited different passwords, 3 passwords for attempt and just one minute blocking between the attempts.  Which can make his impersonation easier. |
| 6 | Use dictatory of common passwords | **Tampering with data**  The common passwords table is not getting updated (we use a table that we first download when we created the system and don’t use API that updated every time with new common passwords. |
| 7 | Save history of 3 passwords | **Spoofing**  Save only history of 3 passwords, so someone that found out a specific old password of one of the user can use it. |
| 8 | Password diversity | **Spoofing**  The user can use the same password throughout the use of the system, he is not requested no change his password every so often, what make it easier for Eve. |
| 9 | Email authentication | **Tampering with data**  There is no email authentication in the registration. User can add any email we want, without check if the email is valid.  (There is validation of valid mail, but no if there is actually mail like this.) |
| 10 | Handling system crash | **Denial of service**  there is no restriction on creating users from a specific computer, what can make the server crash. |

By – Zohar Hazani, Rotem Mor-Haim, Lior Shlomo, Yoni Yirmiyahu, Amit Hadad

😊