We analyzed each one of our vulnerabilities using the STRIDE and DREAD model.

Dread model:

- Damage – how bad would an attack be?
- Reproducibility – how easy is it to reproduce the attack?
- Exploitability – how much work is it to launch the attack?
- Affected users – how many people will be impacted?
- Discoverability – how easy is it to discover the threat?

Each threat in our DREAD model is rated between 1 to 3 in all 5 categories. The DREAD model says that cyber threats with a rating of five to seven are considered a low risk, while cyber threats with a rating of eight to 11 are medium risk. If a cyber threat has a rating of 12 to 15, on the other hand, it’s considered a high risk.

S – Spoofing:

1. An attacker can launch an sql injection in the “search users by name” field, which causes the system to retrieve all the customers, even those the current user should not see. Moreover, this attack can lead to a situation that the entire database is being deleted, or parts from it.

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sevirity
1	2	2	2	1	1	8	Medium
2	1	2	2	1	1	7	Low
3	3	1	1	3	2	10	Medium

T – Tampering:

1. An attacker can launch an sql injection in the “search users by name” field, which causes the system to retrieve all the customers, even those the current user should not see. Moreover, this attack can lead to a situation that the entire database is being deleted, or parts from it.
2. An XSS attack can cause the other users in the system to be spoofed with the malicious JavaScript injected code. This is done by saving a malicious data in the database, which changes the system’s behavior.
3. An attacker can launch sql injection attack in the login page, which will cause a creation of malicious user with high privileges.

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sevirity
1	2	2	3	3	2	12	high
2	3	2	3	3	2	13	high
3	2	2	1	2	1	8	medium

R – Repudiation:

1. An attacker can launch an sql injection in the “search users by name” field, which causes the system to retrieve all the customers, even those the current user should not see. Moreover, this attack can lead to a situation that the entire database is being deleted, or parts from it.
2. An XSS attack can cause the other users in the system to be spoofed with the malicious JavaScript injected code. This is done by saving a malicious data in the database, which changes the system’s behavior.
3. An attacker can launch sql injection attack in the login page, which will cause a creation of malicious user with high privileges.

<u>Note that this attack can be solved with a validation check on the input</u>

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sivirity
1	1	2	2	1	2	8	medium
2	3	1	1	2	2	9	medium
3	2	3	2	3	2	12	high

I - Information disclosure:

1. An attacker can launch an sql injection in the “search users by name” field, which causes the system to retrieve all the customers, even those the current user should not see. Moreover, this attack can lead to a situation that the entire database is being deleted, or parts from it.
2. An XSS attack can cause the other users in the system to be spoofed with the malicious JavaScript injected code. This is done by saving a malicious data in the database, which changes the system’s behavior. NOTE that in this attack the malicious code can be used to send sensitive data from the victims to the attacker.

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sevirity
1	2	3	3	2	1	11	medium
2	3	3	3	3	1	13	High
3	2	3	2	3	2	12	High

D – Denial Of Service:

1. An attacker can launch an sql injection in the “search users by name” field, which causes the entire database to be deleted. In that way a denial of service can be executed.
2. An XSS attack can cause the other users in the system to be spoofed with the malicious JavaScript injected code. This is done by saving a malicious data in the database, which changes the system’s behavior. NOTE that in this attack the malicious code can be used to denial the access of users to the server (from the victims side).

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sevirity
1	1	2	2	2	3	10	Medium
2	2	2	2	2	3	11	Medium
3	2	3	3	2	2	12	High

E – Elevation Of Privilege:

1. An attacker can launch sql injection attack in the login page, which will cause a creation of malicious user with high privileges.

Threat #	D(amage Potential)	R(eproducibility)	E(xploitability)	A(ffected)	D(iscoverability)	Total	Sevirity
1	1	2	1	2	3	9	Medium
2	2	2	1	2	3	10	Medium
3	3	1	1	2	2	9	Medium