**Spoofing**

Spoofing mitigations involve strong authentication mechanisms, including complex password requirements, two-factor authentication, requiring HTTPS, and slow password hashes. A secure implementation of eCommerce applications would enforce strong password complexity requirements by avoiding the commonly used passwords and requiring long and alphanumeric passwords. Requiring a secure web transfer protocol like HTTPS should be a minimum as well. For added security, requiring two-factor authentication when performing susceptible activities such as password changes and any modifications are helpful.

Magento allows different configurations for password requirements, leaving the specific parameters open to the administrators to add. It uses the email template to change the password and the recovery link can be set by admin. Magento does support the use of third-party authentication mechanisms, which is the only way to implement a two-factor authentication approach. Magento requires two-factor authentication for all sensitive administrator-level changes.

**Tampering**

Mitigations for tampering most commonly include the sanitization of input data and authorization mechanisms.

A secure Magento program should have input validation involving datatypes, length, character types, and an approved list validation approach.

**Repudiation**

Magento maintains a log record of all access, which can alert certain threats.

**Information disclosure**

Magento uses Session tokens to authenticate the access and uses an advanced encryption mechanism to protect the information.

**Denial of service**

* Magento implements reverse proxy to allow authorized access.
* Magento has strong access control mechanisms to prevent unnecessary data flow between the trust boundaries
* Magento maintains the sessions timeout which can be handled by admin.
* Magento has controllers and helpers (Fastly) inside the application which can provide services such as CDN, DDoS protection, web application firewall, SSL/TLS certificates, Origin cloaking, image optimization. (https://devdocs.magento.com/cloud/cdn/cloud-fastly.html https://devdocs.magento.com/cloud/cdn/cloud-fastly.html)

**Elevation of Privilege**

Standard mitigation strategies for Elevation of Privilege type threats typically include the following.

* Input validation
* Access control lists, Roles, and Groups
* Ensuring the least amount of access and information is available for given users or system process actions in the context of Magento, there are two different types of privilege elevation, those done within the system and those within the machine the system is running on. For Magento, the application itself and associated processes do not need to be run with admin privileges so we do not concern ourselves with that aspect.

**Reflection**

We have started this assignment by assigning each team member to create a level 0, level 1 DFD from the use case and misuse case scenario developed as part of milestone 2 previously. After finishing the DFD draft, we together discussed the created DFD diagrams and provided feedback for all the DFD diagrams. While doing that, the team discovered a few questions about how to construct the DFDs and that some diagrams had the same structure, since we were not sure what to do, we waited to have the meeting with the professor to continue the project.

After the meeting with the professor, we have clarified our doubts and received some positive feedback and improvement suggestions. Once we are done with the professor meeting, we had another meeting to merge-common DFDs and combined them. Having regular meetings on time for a longer duration making us to complete the assignment on time. Since we merged some DFDs we decided to create groups to treat their threats and create a summary draft. We suffer some problems with the threat’s generation for two DFDs, where two members were not able to generate the threats on their machines. The problem was solved by creating the same DFDs on a different member machine. In the end, we got together to check the threat’s justifications and combine our findings to create the summary.

In this assignment, the team organization improved comparing to the previous ones, and we could see that by how the meetings were organized and the time needed for them. The only problem encountered was the threat generation problem in some DFDs, however, this was countered by working together as a team.