**Spoofing:**

One of the most vital areas in Magento is the Admin Panel, as it has high privileged access to the site. Magento super admin will have full administrator privileges to manage all the functionalities, which includes having full permissions, access to all features and options. Magento Admin’s activities involve handling orders, preparing catalog, arrangement of shipments, CMS, design of storefront, organizing customer information, and managing configurations. Using standard authentication protocols will mitigate spoofing attacks. Magento uses a strong authentication mechanism with two-factor authentication and once authenticated then only the admin can access the Magento catalog. Magento Admin platform has the proper authentication functionality to login and maintain the application. It uses encrypted password and two-factor authentication techniques to validate the login.

<https://docs.magento.com/user-guide/stores/security-admin.html>

**Tampering:**

Magento allows to validate session variables and does input sanitization as a protective measure against possible session fixation attacks. Admin must set these validations at configuration.

<https://docs.magento.com/user-guide/stores/security-session-validation.html>

**Repudiation:**

Action Log feature in Magento captures every change made by an admin to the catalog. All activities will get captured in the Action Log. Admin can validate any suspicious activity by inspecting the activity logs and protect storefront sites from any interference. Any modification done to the catalog can be observed through these logs.

<https://docs.magento.com/user-guide/system/action-log.html>

**Information Disclosure:**

Magento uses standard security certificates for encryption mechanisms such as SSL which securely validates and encrypts data that travels both ways between the browser (client) and server which prevents information disclosure when crossing trust boundaries.

**Denial Of Service:**

Magento uses resources with greater availability, load balancers, and a timeout policy for every process to mitigate this threat. It uses Nginx which functions as a reverse proxy to allow authorized access.

<https://devdocs.magento.com/guides/v2.3/install-gde/prereq/nginx.html?itm_source=devdocs&itm_medium=search_page&itm_campaign=federated_search&itm_term=nginx>

**Elevation Of Privilege:**

Only authorized admins(Merchants) will have access to Magento Catalog/Inventory and they have strong privileges with a two-factor authentication mechanism to avoid any unwanted access. Magento avoids XSS vulnerabilities by validating and sanitizing the inputs. It also sanitizes dynamic values. This contains input and output processing to avoid XSS attacks. Magento uses Content Security Policies (CSP) to avoid cross-site scripting attacks.

<https://devdocs.magento.com/guides/v2.3/extension-dev-guide/xss-protection.html>

<https://devdocs.magento.com/guides/v2.3/extension-dev-guide/security/content-security-policies.html?itm_source=devdocs&itm_medium=search_page&itm_campaign=federated_search&itm_term=csp>