Threat Modeling Report

Created on 11/15/2020 3:39:08 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

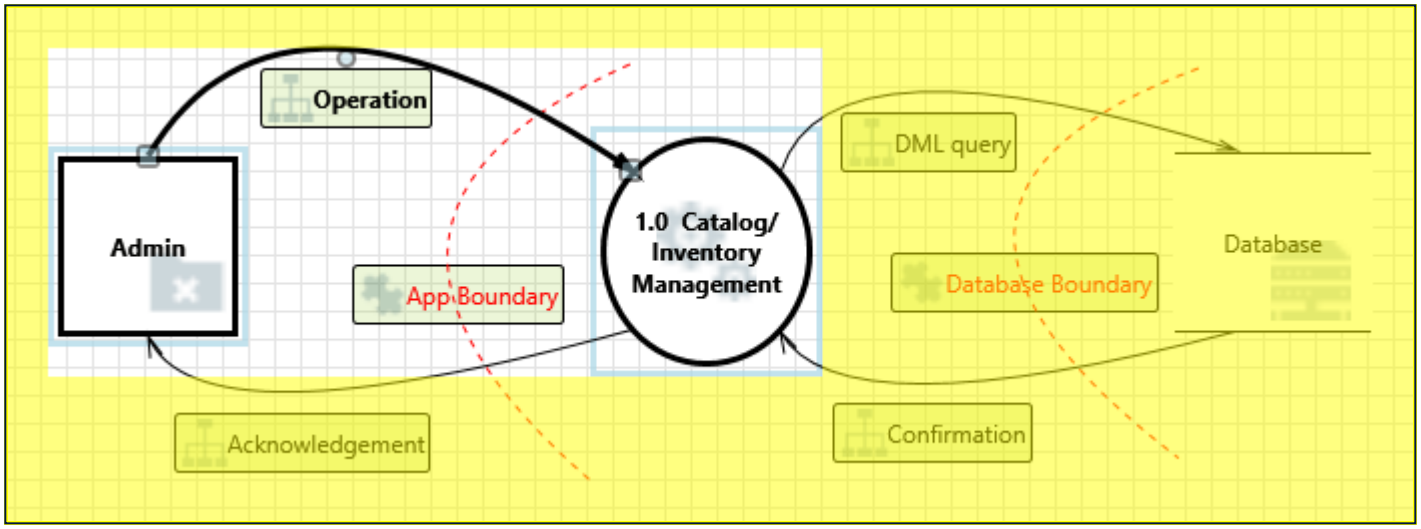
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	14
Total	14
Total Migrated	0

Diagram: Diagram 1



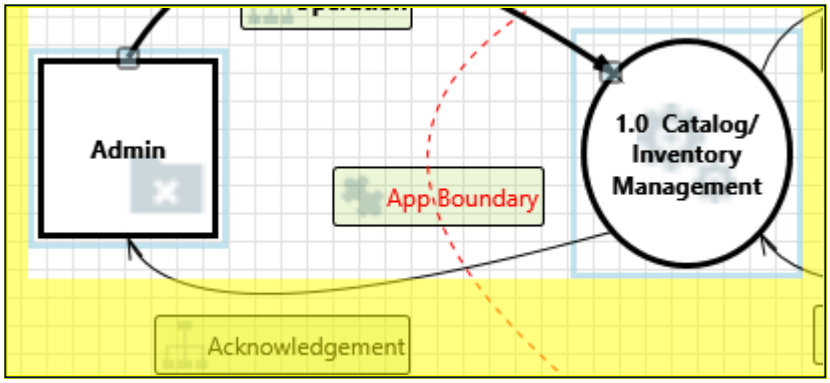
Validation Messages:

1. **Error:** 'Database' requires at least one 'Any'
2. **Error:** The connector should be attached to two elements.
3. **Error:** The connector should be attached to two elements.

Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	14
Total	14
Total Migrated	0

Interaction: Acknowledgement



1. Data Flow Acknowledgement Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: Magento uses Nginx functions as a reverse proxy to allow authorized access.

2. External Entity Admin Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Admin claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: Magento maintains action logs to capture all data modifications.

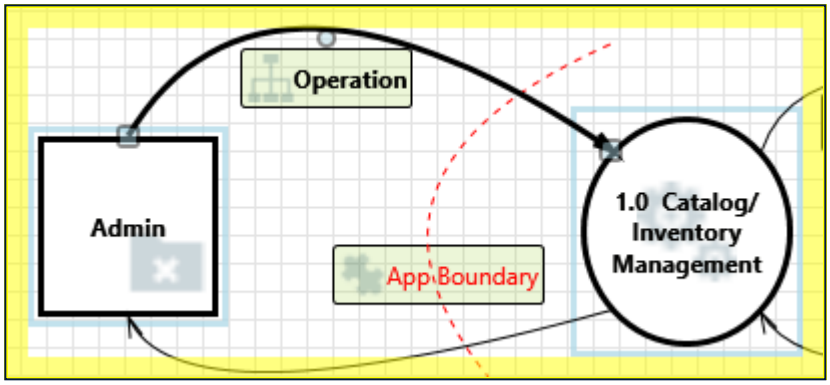
3. Spoofing of the Admin External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Admin may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Admin. Consider using a standard authentication mechanism to identify the external entity.

Justification: Magento uses standard authentication protocols which mitigates spoofing by the attacker.

Interaction: Operation



4. Spoofing the Admin External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Admin may be spoofed by an attacker and this may lead to unauthorized access to 1.0 Catalog/Inventory Management. Consider using a standard authentication mechanism to identify the external entity.

Justification: Uses a strong authentication mechanism and once authentication is passed then only the admin will get access to the Magento catalog.

5. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 Catalog/Inventory Management may be able to impersonate the context of Admin in order to gain additional privilege.

Justification: only authorized admins will have access to Magento Catalog/Inventory and they have strong privileges with a two-factor authentication mechanism to avoid any unwanted access.

6. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web

site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: Magento has input sanitization, XSS prevention, and CSP to avoid cross-site scripting attacks.

7. Elevation by Changing the Execution Flow in 1.0 Catalog/Inventory Management [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 Catalog/Inventory Management in order to change the flow of program execution within 1.0 Catalog/Inventory Management to the attacker's choosing.

Justification: Magento has a secure authorization mechanism at each stage that avoids these threats.

8. 1.0 Catalog/Inventory Management May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Admin may be able to remotely execute code for 1.0 Catalog/Inventory Management.

Justification: Magento allows admin for remote execution only through SSH access.

9. Data Flow Operation Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Magento uses Nginx functions as a reverse proxy to allow authorized access.

10. Potential Process Crash or Stop for 1.0 Catalog/Inventory Management [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: 1.0 Catalog/Inventory Management crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Magento uses resources with greater availability, load balancers and a timeout policy for every

process mitigates this threat.

11. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Operation may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: Magento uses standard encryption mechanisms such as SSL which securely validates and encrypts data that travels both ways between the browser (client) and server.

12. Potential Data Repudiation by 1.0 Catalog/Inventory Management [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: 1.0 Catalog/Inventory Management claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Magento maintains action logs to capture the activity performed which contains time, date of modification along with admin_id.

13. Potential Lack of Input Validation for 1.0 Catalog/Inventory Management [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Operation may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 Catalog/Inventory Management or an elevation of privilege attack against 1.0 Catalog/Inventory Management or an information disclosure by 1.0 Catalog/Inventory Management. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: Data validation constraints avoid this threat.

14. Spoofing the 1.0 Catalog/Inventory Management Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: 1.0 Catalog/Inventory Management may be spoofed by an attacker and this may lead to information disclosure by Admin. Consider using a standard authentication mechanism to identify the destination process.

Justification: Uses a strong authentication mechanism and once authentication is passed then only the admin will get access to the Magento catalog.