Threat Modeling Report

Created on 11/15/2020 1:34:59 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	0
Needs Investigation	1
Mitigation Implemented	28
Total	29
Total Migrated	0

Diagram: Diagram 1

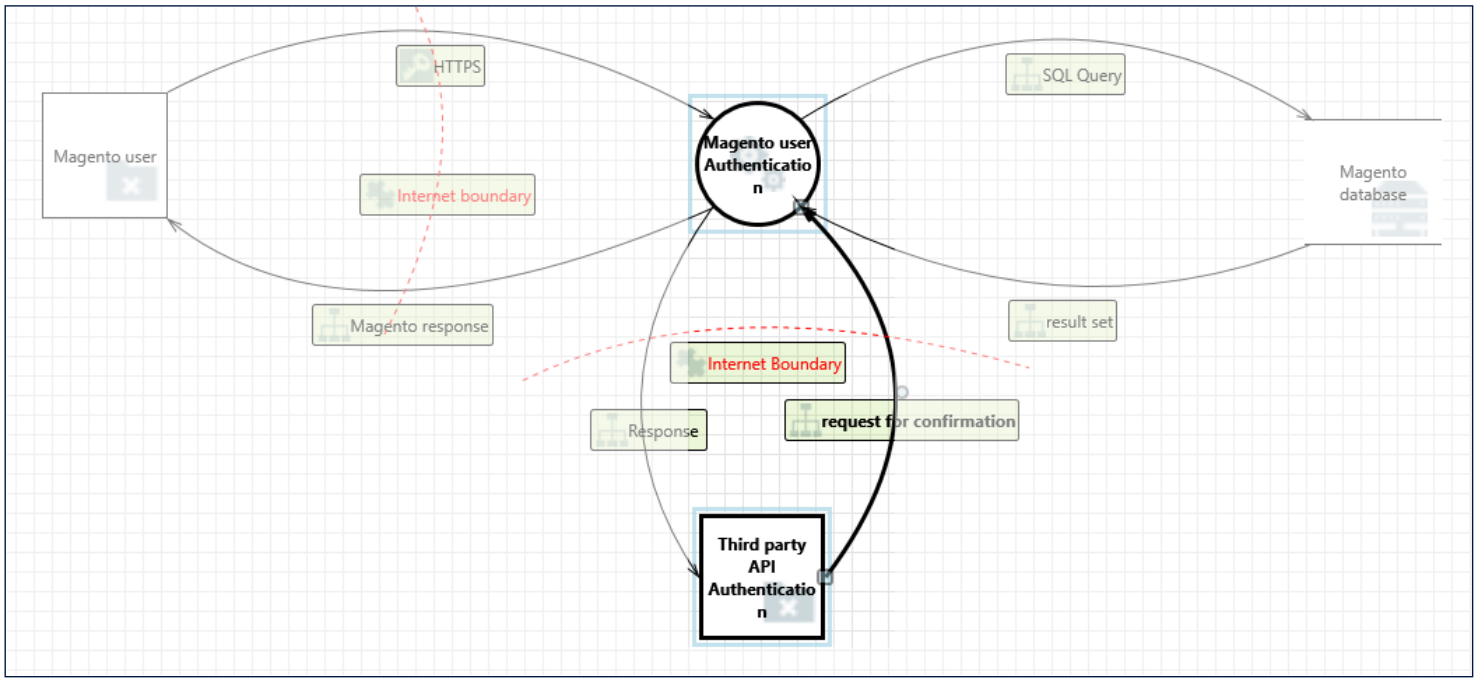
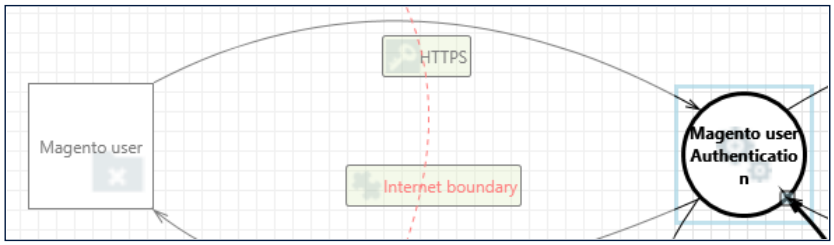


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	0
Needs Investigation	1
Mitigation Implemented	28
Total	29

Total Migrated	0

Interaction: HTTPS



1. Spoofing the Magento user External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Magento user may be spoofed by an attacker and this may lead to unauthorized access to Magento user Authentication. Consider using a standard authentication mechanism to identify the external entity.
Justification: Magento usename and password combination includes Length of password, Special characters inside password and alphanumeric characters which is a standard authentication mechanism

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

Category: Elevation Of Privilege
Description: Magento user Authentication may be able to impersonate the context of Magento user in order to gain additional privilege.
Justification: The users and admins are identified with the URL and authentication process so only the admins are given enough privilege to gain full control

3. Potential Data Repudiation by Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Magento user Authentication 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 the log recording mechanism and alerting mechanism which avoids the all above issues.

4. Potential Process Crash or Stop for Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Magento user Authentication crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Magento has controllers and helpers (Fastly) inside the application which avoids the above scenarios

5. Data Flow HTTPS 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 implements reverse proxy to allow authorized access.

6. Magento user Authentication May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Magento user may be able to remotely execute code for Magento user Authentication.
Justification: Magento only allows admin to remotely execute code through SSH.

7. Elevation by Changing the Execution Flow in Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Magento user Authentication in order to change the flow of program execution within Magento user Authentication to the attacker's choosing.
Justification: Magento implements secure authorization mechanisms at every phase

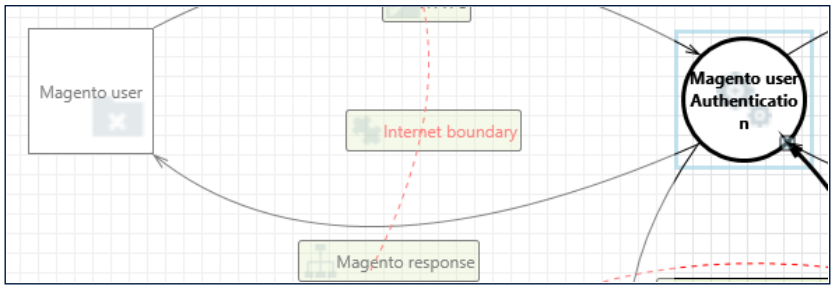
8. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

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 recommends user to set up security configurations such as avoid sending server version, cleaning the server header, disallowing trace requests, securing the cookies when using SSL. It also prevents cross-site scripting and allows user to set a timeout.

Interaction: Magento response



9. Spoofing of the Magento user External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Magento uses session token authentication mechanisms

10. External Entity Magento user Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Magento user 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 uses session token authentication mechanisms

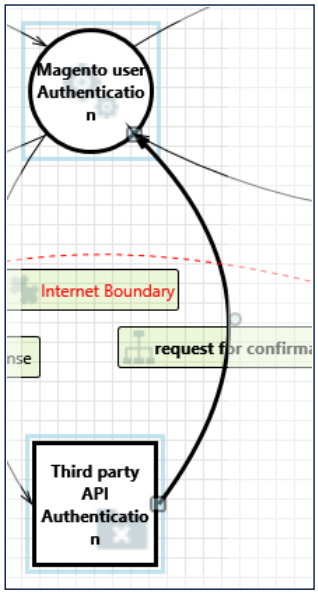
11. Data Flow Magento response Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

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

Justification: Magento implements reverse proxy to allow authorized access.

Interaction: request for confirmation



12. Spoofing the Third party API Authentication External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Third party API Authentication may be spoofed by an attacker and this may lead to unauthorized access to Magento user Authentication. Consider using a standard authentication mechanism to identify the external entity.
Justification: Magento allows any actions to be performed only after proper authentication, It implements ACL model.

13. Spoofing the Magento user Authentication Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Magento user Authentication may be spoofed by an attacker and this may lead to information disclosure by Third party API Authentication. Consider using a standard authentication mechanism to identify the destination process.
Justification: Magento uses session token authentication mechanisms

14. Potential Lack of Input Validation for Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across request for confirmation may be tampered with by an attacker. This may lead to a denial of service attack against Magento user Authentication or an elevation of privilege attack against Magento user Authentication or an information disclosure by Magento user Authentication. 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: Magento secures data by using industry-standard Advanced Encryption Standard (AES-256) algorithm and Secure Hash Algorithm (SHA-256) is used to hash all data that does not require decryption.

15. Potential Data Repudiation by Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Magento user Authentication 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 log recording meachanism and alerting mechanism to avoid the above issues

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

Category: Information Disclosure
Description: Data flowing across request for confirmation 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 provides advance encryption mechanisms.

17. Potential Process Crash or Stop for Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Magento user Authentication crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Magento has controllers and helpers (Fastly) inside the application which can take care of the above.

18. Data Flow request for confirmation 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 has strong access control mechanisms in order to prevent unnecessary data flow between the trust boundaries

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

Category: Elevation Of Privilege
Description: Magento user Authentication may be able to impersonate the context of Third party API Authentication in order to gain additional privilege.
Justification: The Third party Authentication uses OAuth protocol follows all standards which avoids all additional privileges.

20. Magento user Authentication May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Third party API Authentication may be able to remotely execute code for Magento user Authentication.
Justification: Magento only allows admin to remotely execute code through SSH.

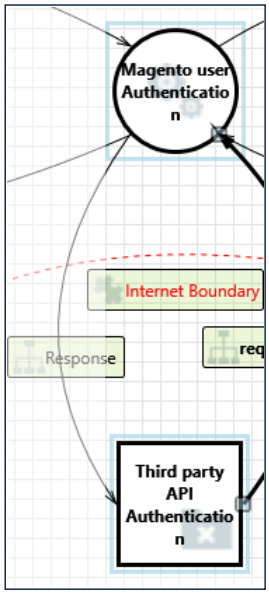
21. Elevation by Changing the Execution Flow in Magento user Authentication [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Magento user Authentication in order to change the flow of program execution within Magento user Authentication to the attacker's choosing.
Justification: Magento implements secure authorization mechanisms at every phase (session token)

22. 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 recommends user to set up security configurations such as avoid cleaning the server header, disallowing trace requests, securing the cookies when using SSL. It also prevents cross-site scripting and allows user to set a timeout.

Interaction: Response



23. Data Flow Response 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 has strong access control mechanisms in order to prevent unnecessary data flow between the trust boundaries.

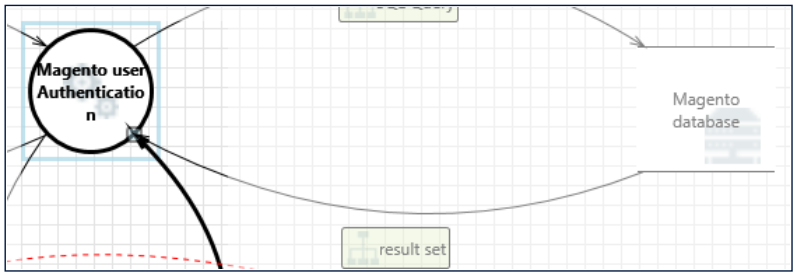
24. External Entity Third party API Authentication Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Third party API Authentication 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 a log record for all its Third party authentications

25. Spoofing of the Third party API Authentication External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Third party API Authentication may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Third party API Authentication. Consider using a standard authentication mechanism to identify the external entity.
Justification: Magento allows any actions to be performed only after proper authentication, It implements ACL model.

Interaction: result set



26. Spoofing of Source Data Store Magento database [State: Needs Investigation] [Priority: High]

Category: Spoofing
Description: Magento database may be spoofed by an attacker and this may lead to incorrect data delivered to Magento user Authentication. Consider using a standard authentication mechanism to identify the source data store.
Justification: <no mitigation provided>

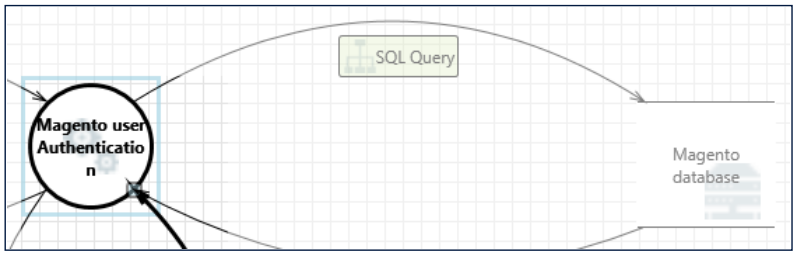
27. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Magento database can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: Magento provides standard third party authentication techniques using tokens.

Interaction: SQL Query



28. Spoofing of Destination Data Store Magento database [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Magento database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Magento database. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Magento uses SSL and AES authentication mechanisms to avoid attacker getting info from the Magento

29. Potential Excessive Resource Consumption for Magento user Authentication or Magento database [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Magento user Authentication or Magento database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Magento maintains the sessions timeout which can be handled by admin.