Threat Modeling Report

Created on 11/14/2022 12:51:33 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

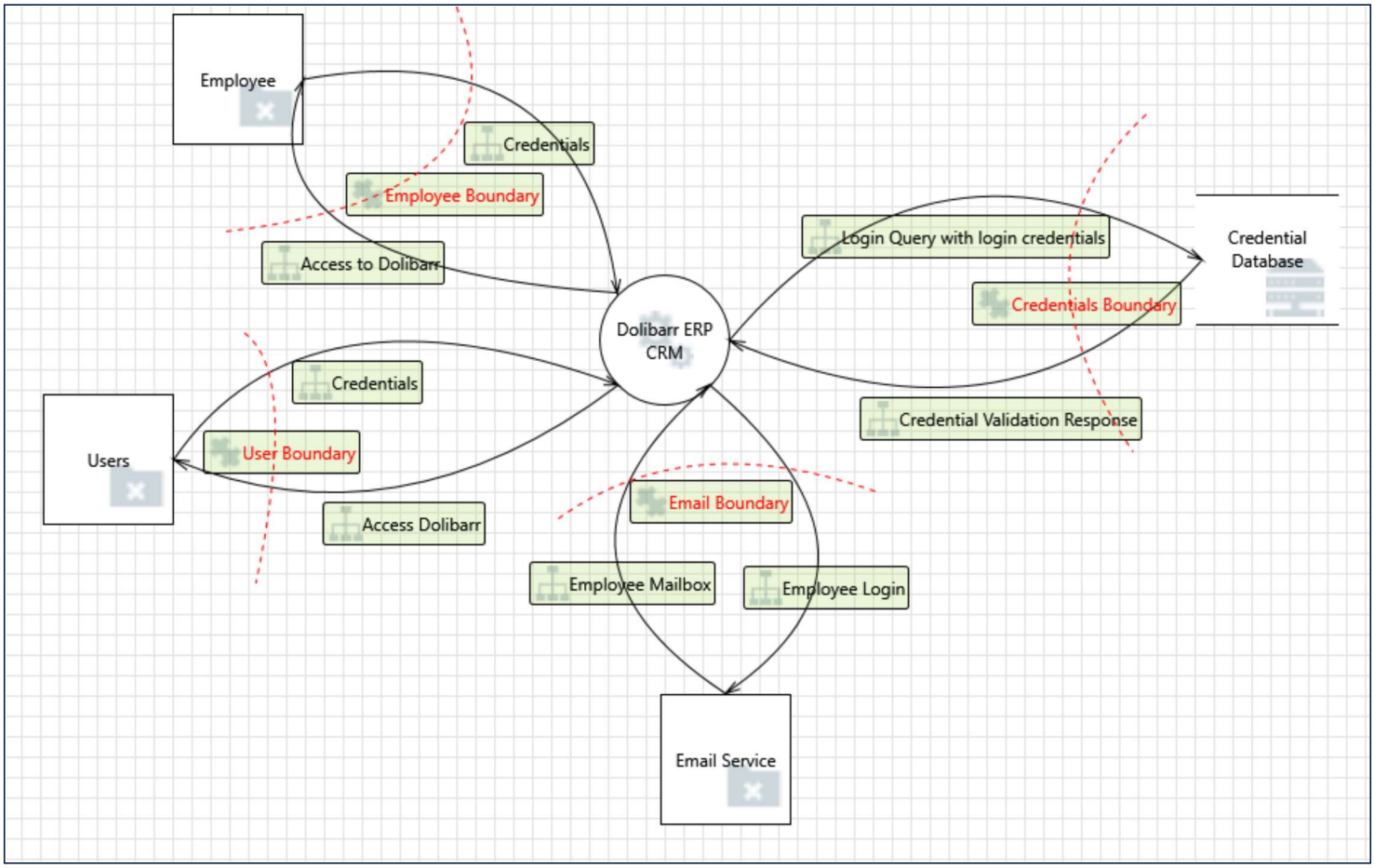
Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	4
Needs Investigation	5
Mitigation Implemented	50
Total	59
Total Migrated	0

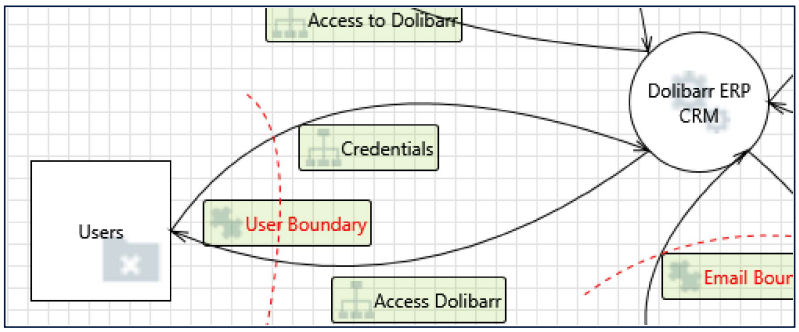
Diagram: Time Sheet Data



Time Sheet Data Diagram Summary:

Not Started	0
Not Applicable	4
Needs Investigation	5
Mitigation Implemented	50
Total	59
Total Migrated	0

Interaction: Access Dolibarr



1. Spoofing of the Users External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Dolibarr has strong authentication policies.

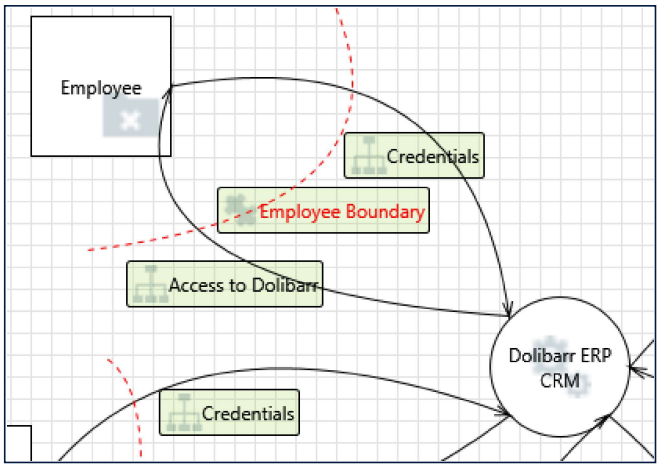
2. External Entity Users Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Users 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: We discovered indications of a log for login attempts in the Dolibarr documentation.

3. Data Flow Access Dolibarr Is Potentially Interrupted [State: Needs Investigation] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: A Denial of Service on a user login should be possible for a system administrator.

Interaction: Access to Dolibarr



4. Spoofing of the Employee External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Employee may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Employee. Consider using a standard authentication mechanism to identify the external entity.
Justification: Dolibarr has strong authentication policies.

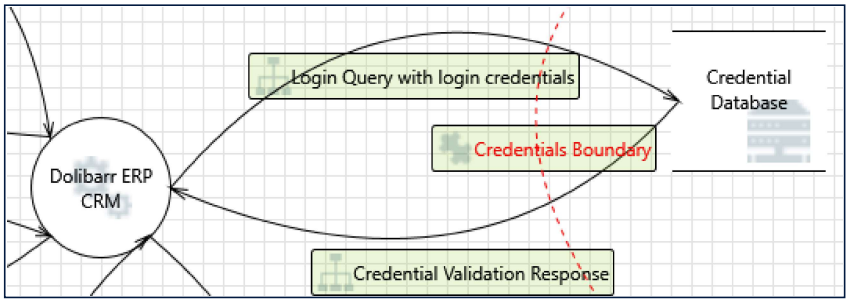
5. External Entity Employee Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Employee 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: We discovered indications of a log for login attempts in the Dolibarr documentation.

6. Data Flow Access to Dolibarr Is Potentially Interrupted [State: Needs Investigation] [Priority: High]

Category: Denial Of Service
Description: An external agent interrupts data flowing across a trust boundary in either direction.
Justification: A Denial of Service on an Employee login should be possible for a system administrator.

Interaction: Credential Validation Response



7. Spoofing of Source Data Store Credential Database [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Credential Database may be spoofed by an attacker and this may lead to incorrect data delivered to Dolibarr ERP CRM. Consider using a standard authentication mechanism to identify the source data store.
Justification: Spoofing is not possible because of the Internal database.

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

Category: Information Disclosure
Description: Improper data protection of Credential Database can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: Input Validation and User access Controls

9. Spoofing the Dolibarr ERP CRM Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Dolibarr ERP CRM may be spoofed by an attacker and this may lead to information disclosure by Credential Database . Consider using a standard authentication mechanism to identify the destination process.
Justification: Internal Database

10. Potential Data Repudiation by Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Dolibarr ERP CRM 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: Dolibarr Tracks all the user actions and generates logs when required

11. Potential Process Crash or Stop for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Dolibarr ERP CRM crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Restarting the Dolibarr System should be possible for a system administrator.

12. Data Flow Credential Validation 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: It's an Internal process.

13. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Internal Database can't be made Inaccessible

14. Dolibarr ERP CRM May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Credential Database may be able to remotely execute code for Dolibarr ERP CRM.

Justification: Input Validation

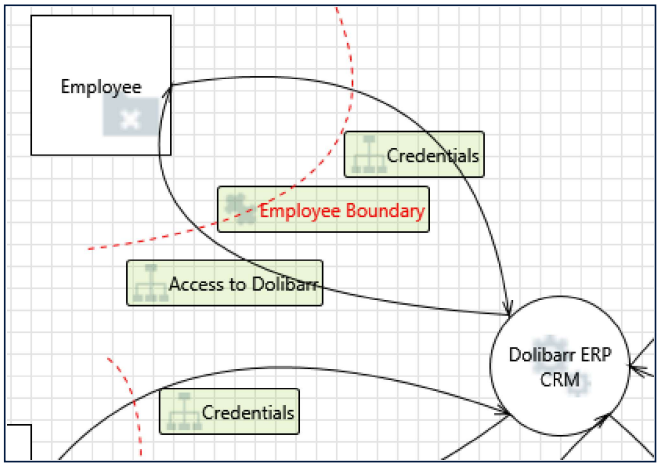
15. Elevation by Changing the Execution Flow in Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Dolibarr ERP CRM in order to change the flow of program execution within Dolibarr ERP CRM to the attacker's choosing.

Justification: Input Validation.

Interaction: Credentials



16. Spoofing the Employee External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Employee may be spoofed by an attacker and this may lead to unauthorized access to Dolibarr ERP CRM. Consider using a standard authentication mechanism to identify the external entity.

Justification: Dolibarr Authentication Process.

17. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Dolibarr ERP CRM may be able to impersonate the context of Employee in order to gain additional privilege.

Justification: <no mitigation provided>

18. Spoofing the Dolibarr ERP CRM Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Dolibarr ERP CRM may be spoofed by an attacker and this may lead to information disclosure by Employee. Consider using a standard authentication mechanism to identify the destination process.

Justification: Dolibarr Authentication Process.

19. Potential Lack of Input Validation for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Credentials may be tampered with by an attacker. This may lead to a denial of service attack against Dolibarr ERP CRM or an elevation of privilege attack against Dolibarr ERP CRM or an information disclosure by Dolibarr ERP CRM. 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: mitigated by input validation and timeout after an excessive number of attempts.

20. Potential Data Repudiation by Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Dolibarr ERP CRM 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: Dolibarr Tracks all the user actions and generates logs when required

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

Category: Information Disclosure
Description: Data flowing across Credentials 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: Dolibarr uses letsencrypt to mitigate this.

22. Potential Process Crash or Stop for Dolibarr ERP CRM [State: Needs Investigation] [Priority: High]

Category: Denial Of Service
Description: Dolibarr ERP CRM crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Restarting the Dolibarr System should be possible for a system administrator.

23. Data Flow Credentials 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: Restarting the Dolibarr System should be possible for a system administrator.

24. Dolibarr ERP CRM May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Employee may be able to remotely execute code for Dolibarr ERP CRM.
Justification: User Access Controls are implemented

25. Elevation by Changing the Execution Flow in Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Dolibarr ERP CRM in order to change the flow of program execution within Dolibarr ERP CRM to the attacker's choosing.
Justification: User Access Controls are implemented

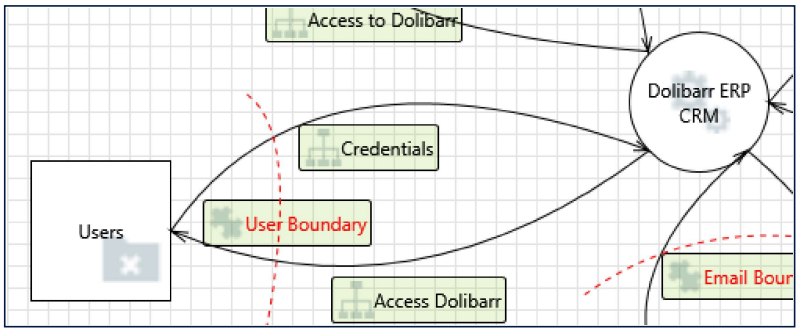
26. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

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: in Dolibarr forms are protected with a CSRF token against CSRF attacks

Interaction: Credentials



27. Spoofing the Users External Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Users may be spoofed by an attacker and this may lead to unauthorized access to Dolibarr ERP CRM. Consider using a standard authentication mechanism to identify the external entity.

Justification: Dolibbarr Authentication process.

28. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Dolibarr ERP CRM may be able to impersonate the context of Users in order to gain additional privilege.

Justification: <no mitigation provided>

29. Spoofing the Dolibarr ERP CRM Process [State: Needs Investigation] [Priority: High]

Category: Spoofing

Description: Dolibarr ERP CRM may be spoofed by an attacker and this may lead to information disclosure by Users. Consider using a standard authentication mechanism to identify the destination process.

Justification: Rigorous training to employees to identify Dolibarr's trusted destinations.

30. Potential Lack of Input Validation for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Credentials may be tampered with by an attacker. This may lead to a denial of service attack against Dolibarr ERP CRM or an elevation of privilege attack against Dolibarr ERP CRM or an information disclosure by Dolibarr ERP CRM. 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: mitigated by input validation and timeout after an excessive number of attempts.

31. Potential Data Repudiation by Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Repudiation
Description: Dolibarr ERP CRM 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: Dolibarr Tracks all the user actions and generates logs when required

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

Category: Information Disclosure
Description: Data flowing across Credentials 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: Dolibarr uses letsencrypt to mitigate this.

33. Potential Process Crash or Stop for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service
Description: Dolibarr ERP CRM crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification: Restarting the Dolibarr System should be possible for a system administrator.

34. Data Flow Credentials 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: Restarting the Dolibarr System should be possible for a system administrator.

35. Dolibarr ERP CRM May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: Users may be able to remotely execute code for Dolibarr ERP CRM.
Justification: User Access Controls are implemented

36. Elevation by Changing the Execution Flow in Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Dolibarr ERP CRM in order to change the flow of program execution within Dolibarr ERP CRM to the attacker's choosing.
Justification: User Access Controls are implemented

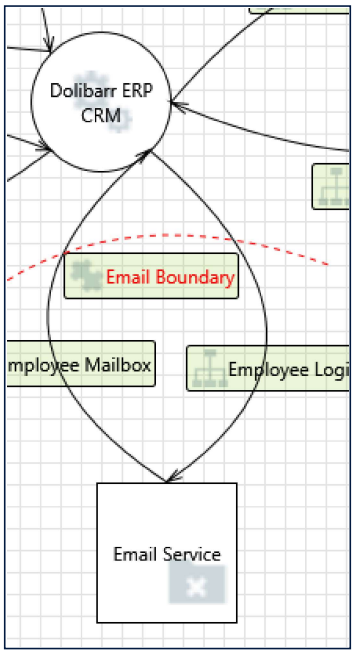
37. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

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: in Dolibarr forms are protected with a CSRF token against CSRF attacks

Interaction: Employee Login



38. Spoofing of the Email Service External Destination Entity [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: Dolibarr has strong authentication to restrict outbound emails.

39. External Entity Email Service Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Email Service 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: We discovered indications of a log for login attempts in the Dolibarr documentation.

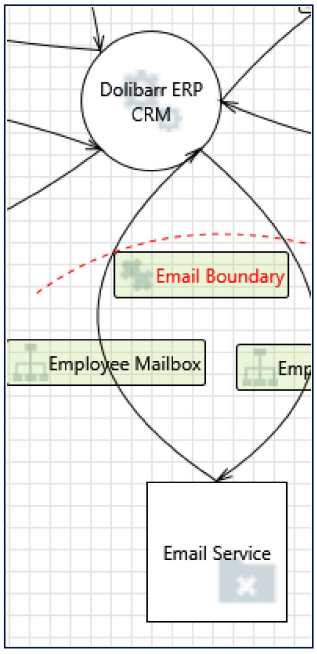
40. Data Flow Employee Login Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

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

Justification: An employee login should be subject to a Denial of Service by a system administrator.

Interaction: Employee Mailbox



41. Spoofing the Email Service External Entity [State: Needs Investigation] [Priority: High]

Category: Spoofing
Description: Email Service may be spoofed by an attacker and this may lead to unauthorized access to Dolibarr ERP CRM. Consider using a standard authentication mechanism to identify the external entity.
Justification: This would be highly dependent on the use of the external mail service and how it integrates with Dolibarr.

42. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege
Description: Dolibarr ERP CRM may be able to impersonate the context of Email Service in order to gain additional privilege.
Justification: <no mitigation provided>

43. Spoofing the Dolibarr ERP CRM Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing
Description: Dolibarr ERP CRM may be spoofed by an attacker and this may lead to information disclosure by Email Service. Consider using a standard authentication mechanism to identify the destination process.
Justification: This is handled using IMAP.

44. Potential Lack of Input Validation for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Tampering
Description: Data flowing across Employee Mailbox may be tampered with by an attacker. This may lead to a denial of service attack against Dolibarr ERP CRM or an elevation of privilege attack against Dolibarr ERP CRM or an information disclosure by Dolibarr ERP CRM. 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: Dolibarr uses SSL and needs that it be present in the mailbox.

45. Potential Data Repudiation by Dolibarr ERP CRM [State: Not Applicable] [Priority: High]

Category: Repudiation
Description: Dolibarr ERP CRM 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: External email service will handle this threat.

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

Category: Information Disclosure

Description: Data flowing across Employee Mailbox 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: This will be mitigated by SSL and IMAP in Dolibarr.

47. Potential Process Crash or Stop for Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Dolibarr ERP CRM crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: Restarting the Dolibarr System should be possible for a system administrator.

48. Data Flow Employee Mailbox 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: This should be handled by email service.

49. Dolibarr ERP CRM May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Email Service may be able to remotely execute code for Dolibarr ERP CRM.

Justification: Dolibarr has strong User Access Controls over code executions.

50. Elevation by Changing the Execution Flow in Dolibarr ERP CRM [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Dolibarr ERP CRM in order to change the flow of program execution within Dolibarr ERP CRM to the attacker's choosing.

Justification: Dolibarr User Access Controls.

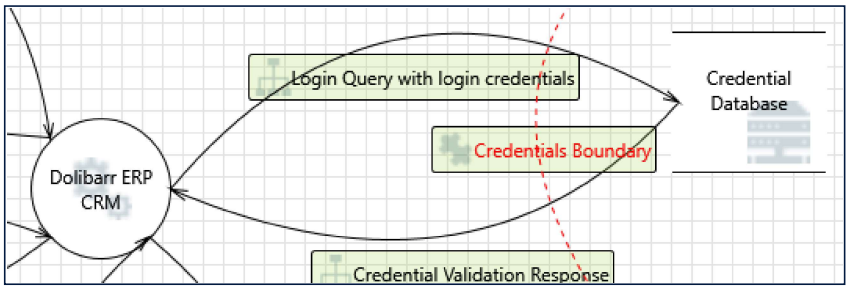
51. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

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: in Dolibarr forms are protected with a CSRF token against CSRF attacks.

Interaction: Login Query with login credentials



52. Spoofing of Destination Data Store Credential Database [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

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

Justification: It will not be allowed to hit the spoof database because it is internal.

53. Potential Excessive Resource Consumption for Dolibarr ERP CRM or Credential Database [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does Dolibarr ERP CRM or Credential 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: Dolibarr uses IP limitation to stop bots from flooding the authentication process and locks out users after a certain number of failed login attempts.

54. Data Store Inaccessible [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: Dolibarr has Internal Datastore.

55. Data Flow Login Query with login credentials 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: It is an Internal Data Store.

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

Category: Information Disclosure

Description: Data flowing across Login Query with login credentials 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: Dolibarr uses letsencrypt to mitigate this.

57. Data Store Denies Credential Database Potentially Writing Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: Credential Database claims that it did not write data received from an entity 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: Dolibarr Tracks all the user actions and generates logs when required

58. The Credential Database Data Store Could Be Corrupted [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across Login Query with login credentials may be tampered with by an attacker. This may lead to corruption of Credential Database . Ensure the integrity of the data flow to the data store.

Justification: There are strong User Access Controls to prevent any unwanted tampering from within the organization, and the database is internal.

59. Spoofing the Dolibarr ERP CRM Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Dolibarr ERP CRM may be spoofed by an attacker and this may lead to unauthorized access to Credential Database . Consider using a standard authentication mechanism to identify the source process.

Justification: The internal process cannot be spoofed without proper authentication.