[SDEA-21] Password Management Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Does the Password Policy enforce Password Complexity requirements like use of passphrase?
2. Is all the Password stored in database are hashed with unique salt value?
3. Does Password recovery and changing operations have the same level of controls as account creation and authentication?

[SDEA-20] File Uploads Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Is the file extension to be uploaded is validated against the whitelist of permitted extensions rather than a blacklist of prohibited ones?
2. Is the file path or file name canonicalized?
3. Does the file uploaded in a sandbox environment and validated before moving it to the server's permanent filesystem?
4. Is an established framework used for preprocessing file uploads rather than attempting to write your own validation mechanisms?

[SDEA-19] Database Security Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Is Parametrized Queries in place to mitigate SQL Injection?
2. Is input validation in place for user inputs to Database?
3. Is least level of privilege in place for an application access the Database?
4. Is encryption of connection string or credentials to access any Database related function is in place?

[SDEA-18] System Configuration Management Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Is the Libraries, Frameworks and system components are patched regularly; is it ensured that they are running the latest approved version?
2. Is generic error messages and custom error messages (not revealing too much of system internals) in place in case of any errors?
3. Is all the exceptions and administrative functions Logged?
4. Is the unnecessary extended HTTP methods disabled?

[SDEA-17] Sensitive Information Storage or Transmission

Created: 05/Nov/23 Updated: 05/Nov/23

Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Is there a strong encryption algorithm in place to protect the data in rest and in transit?
2. Is the logs prevented from having sensitive user information or PII data?
3. Is the developer comments in the source code, unnecessary system documentation and unnecessary application were removed?

[SDEA-16] Session Management Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Does the session tokens have the sufficient random entropy?
2. Does the cookies generated from the server side is transmitted over the secure connection and has the “Secure” and “HttpOnly” attributes enabled.
3. Does a sensitive server side operations utilize per-session random tokens like Anti CSRF tokens to prevent Cross Site Request Forgery attacks?

[SDEA-14] Authentication and Authorisation Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. How do users and other actors in the system, including clients and servers, authenticate each other so that there is a guarantee against impersonation?
2. Do all operations in the system require authorization, and are these given to only the level necessary, and no more (for example a user accessing a database has limited access to only those tables and columns they really need access to)?
3. Is access granted in a role-based fashion? Are all access decisions relevant at the time access is performed? (token/permissions updated with state-changing actions; token/permissions checked before access is granted).
4. Are all objects in the system subject to proper access control with the appropriate mechanisms (files, web pages, resources, operations on resources, etc.)?
5. Is access to sensitive data and secrets limited to only those who need it?
6. Is all the authentication and access events (be it successful or failed attempt) is being logged?

[SDEA-13] Data Validation Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Epic Link:	Secure Design
Sprint:	

Description

1. Is all the user inputs from the client side such as form fields, URLs and HTTP Header values or data from the external system is validated?
2. Based on the context, Is all the data output to the client is Encoded?
3. Are the Framework supported Libraries used for Validation and Encoding rather than writing a customized one?

[SDEA-12] Injection Created: 05/Nov/23 Updated: 05/Nov/23	
Status:	To Do
Project:	Secure Design of Ecommerce Application
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Story	**Priority:**	Medium
Reporter:	Aishwarya Selvarajan	**Assignee:**	Unassigned
Resolution:	Unresolved	**Votes:**	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Sprint:	

Generated at Sun Nov 05 17:16:25 UTC 2023 by Aishwarya Selvarajan using Jira 1001.0.0-SNAPSHOT#100240-sha1:341642299face3a73787b1ff0621c4c5fa6e6142.