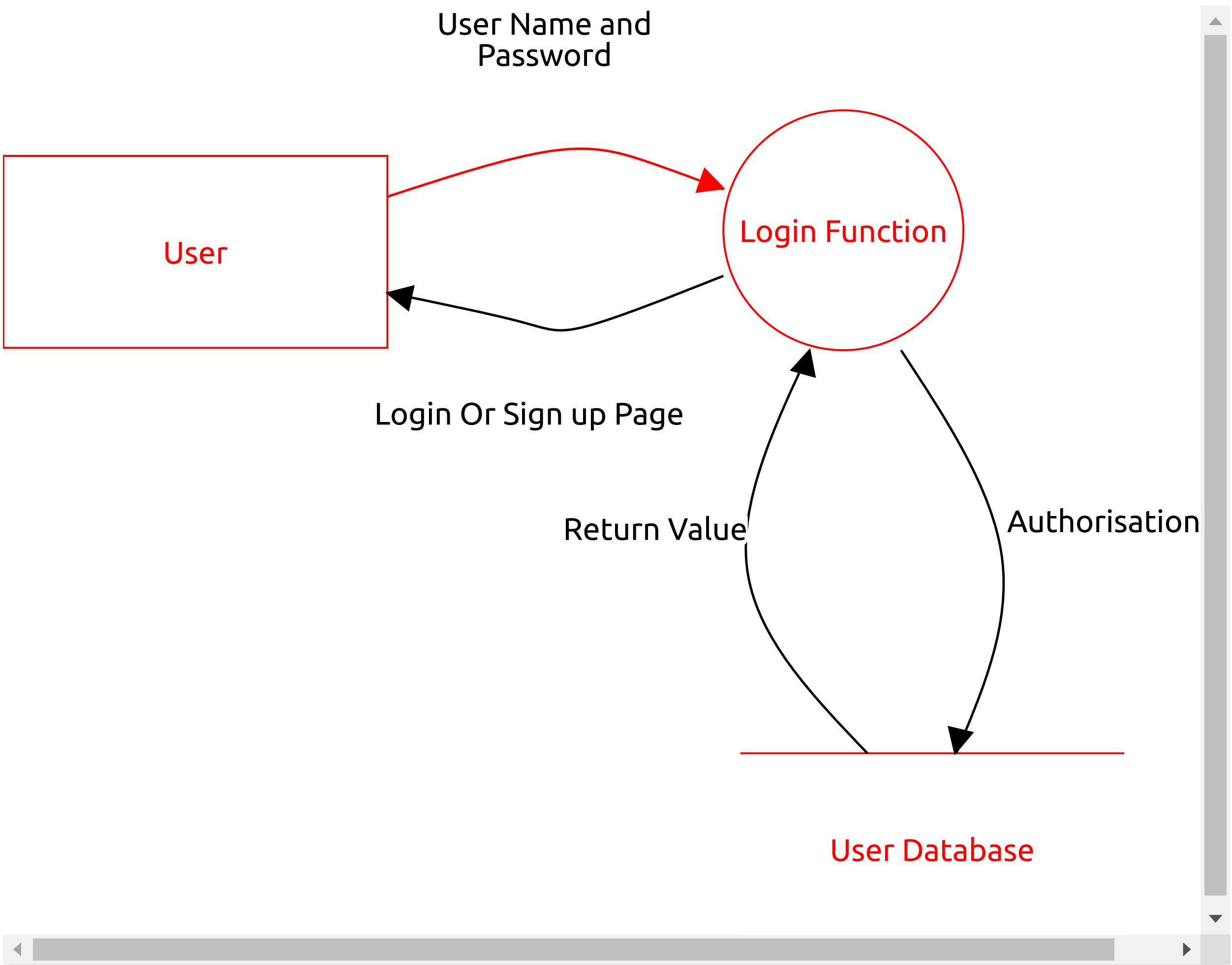
Threat model report for Food Order Application Threat Model

Owner:
Joshua
Reviewer:
Contributors:

High level system description

This is the threat model created for the food ordering application with the Following Scenarios
- Login Functionality
- Payment Functioanality
- Search For Food
- Pro User

Login



User (External Actor)

Description:

Spoofing as admin

Spoofing, Open, Medium Severity

Description:
Some times the Attacker may try to login using the Leaked admin credential

Mitigation:
Add multifactor Authentication

Login Function (Process)

Description:

No Logs for Login

Repudiation, Open, High Severity

Description:
The Login Function has no attribute to store the logs this leaves no trace when the attacker try to use the User account and make some changes

Mitigation:
There should be the Log mechanism added to the Login Functionality

User Database (Data Store)

Description:
Database that Stores the User credential

Information Leakage

Information disclosure, Open, Medium Severity

Description:
The Information stored in the user credential DB leaked using the SQL injection in the Login Page

Mitigation:
Use paramterized query to remediate the Issue

User Name and Password (Data Flow)

Description:

Man In the Middle Attack

Information disclosure, Open, Medium Severity

Description:
The attacker may perform man In the Middle attack and retrives the User credentials

Mitigation:
Use Safe tranmission mechanism like HTTPS to tranfer the information

Too much Login Attempt

Denial of service, Open, Medium Severity

Description:
The attacker may perform Too much login attempt and makes the server down

Mitigation:
Load balancer should be Used in front of the Server

Account Takeveover using Bruteforcing

Elevation of privilege, Open, Medium Severity

Description:
The attacker may perfrom bruteforcing on the user account to guess the password

Mitigation:
Rate Limiting Should be implemeneted at the Login Page

Authorisation (Data Flow)

Description:
Check for

No threats listed.

Return Value (Data Flow)

Description:

The flow will return whether the user is registered or new user based on the result

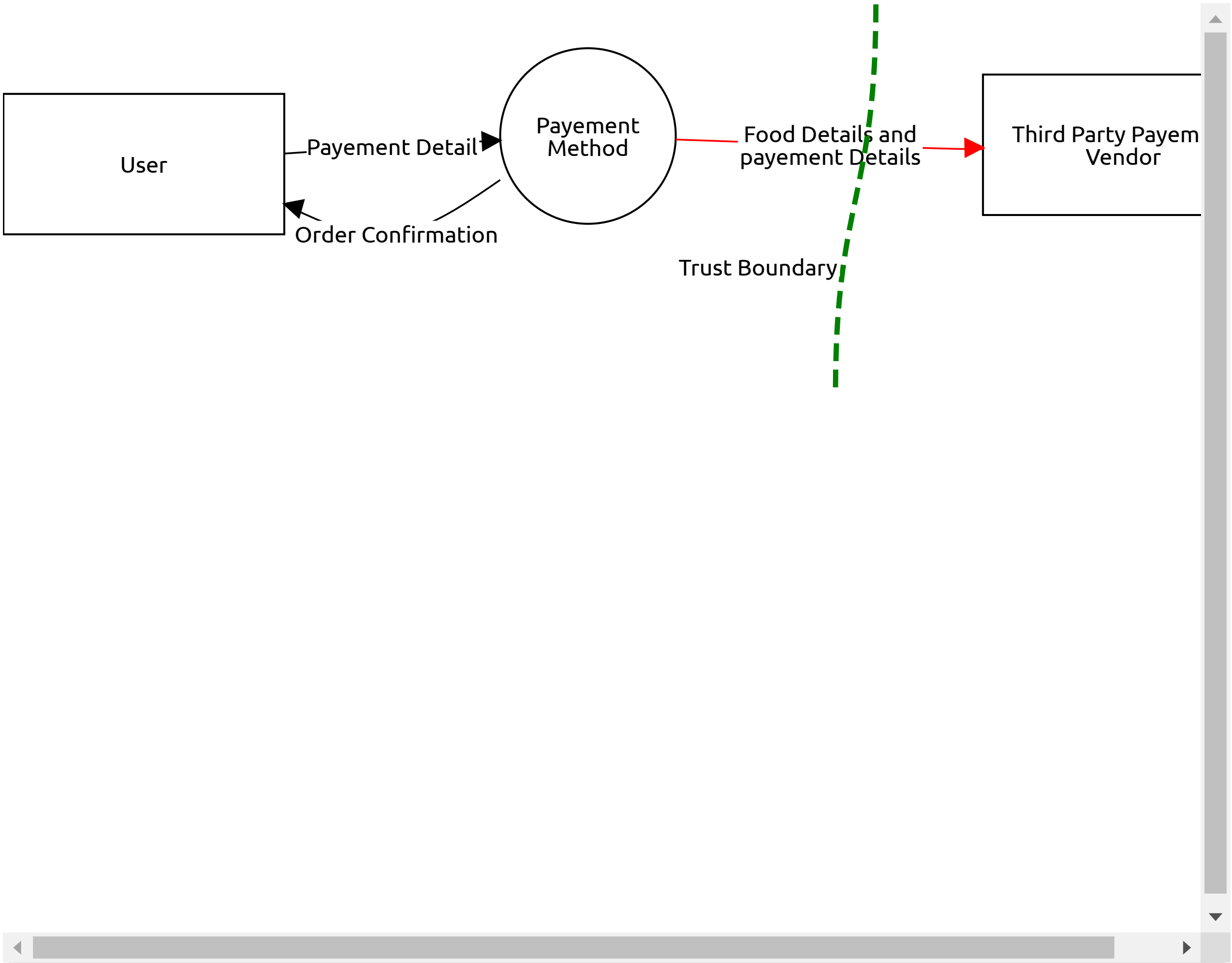
No threats listed.

Login Or Sign up Page (Data Flow)

Description:
Based on the result It shows Login or Sign Up Page

No threats listed.

Payment



User (External Actor)

Description:

No threats listed.

Payement Method (Process)

Description:

No threats listed.

Third Party Payement Vendor (External Actor)

Description:

No threats listed.

Payement Detail (Data Flow)

Description:

No threats listed.

Food Details and payement Details (Data Flow)

Description:

Price Changing

Tampering, Open, Medium Severity

Description:
The attacker may tamper the price of the food using the proxy like burp and zap

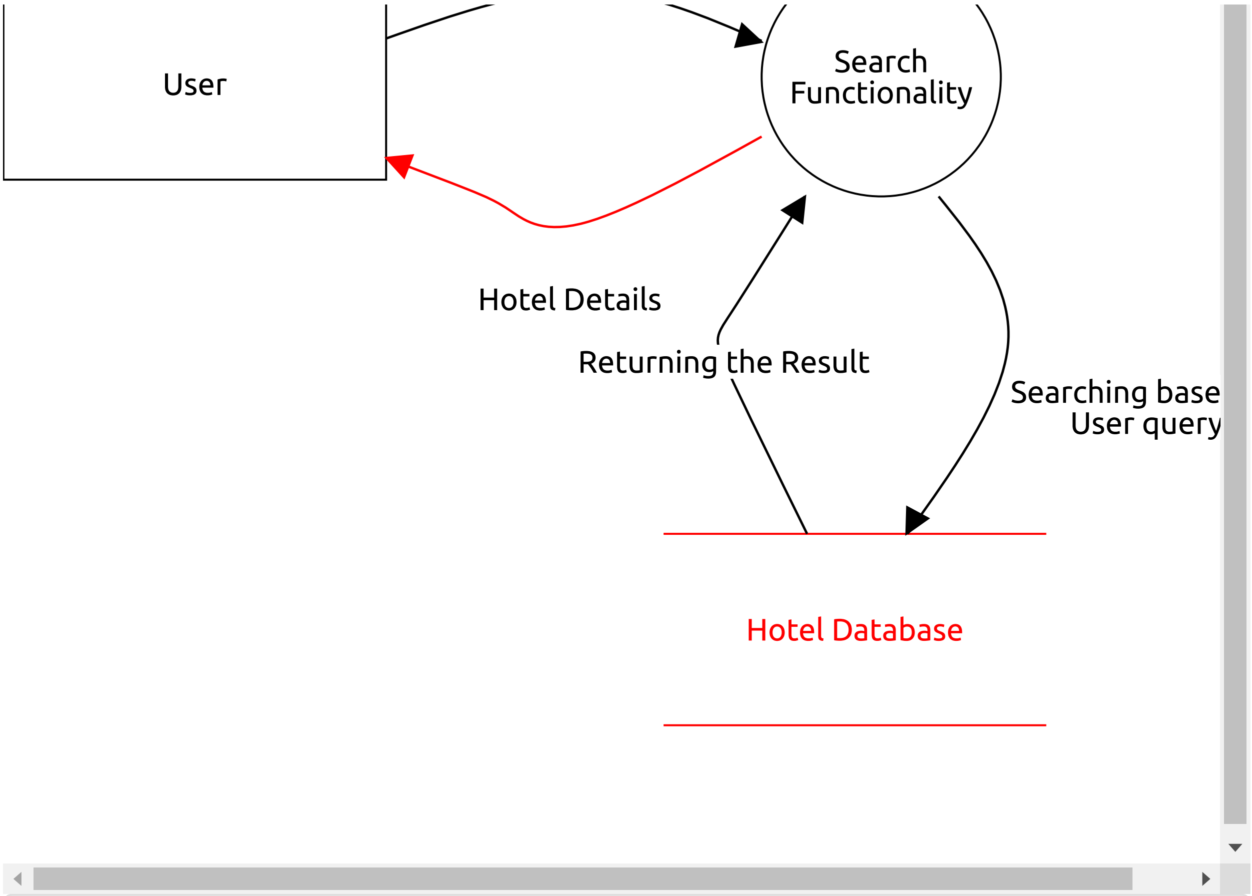
Mitigation:
The server should validate the integrity of the request by Digital Signature and Hashes

Order Confirmation (Data Flow)

Description:

No threats listed.

Search For Food



User (External Actor)

Description:

No threats listed.

Search Functionality (Process)

Description:

No threats listed.

Hotel Database (Data Store)

Description:
This Database consist to hotel and their menu items

Create the Hotels with Similar Same

Spoofing, Open, Medium Severity

Description:
Sometimes the attackers may create the Similar hotels name to Scam the People

Mitigation:
Only Verified owners or authorised person should only allowed to make the Change

Hotel Name or Food Name (Data Flow)

Description:
Search for Hotel or foods based on the User query

No threats listed.

Hotel Details (Data Flow)

Description:

Tampering the result With the False Result

Tampering, Open, Medium Severity

Description:
The attacker may result tamper the result and show the food with more price or poor food with the good reviews

Mitigation:
Validating the response message Integrity using the Digital Signature and Hashing

Searching based on User query (Data Flow)

Description:

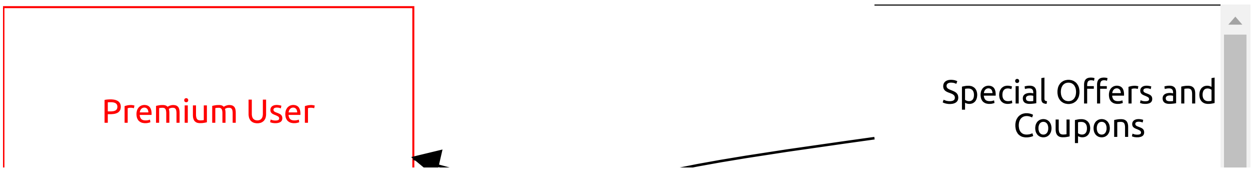
No threats listed.

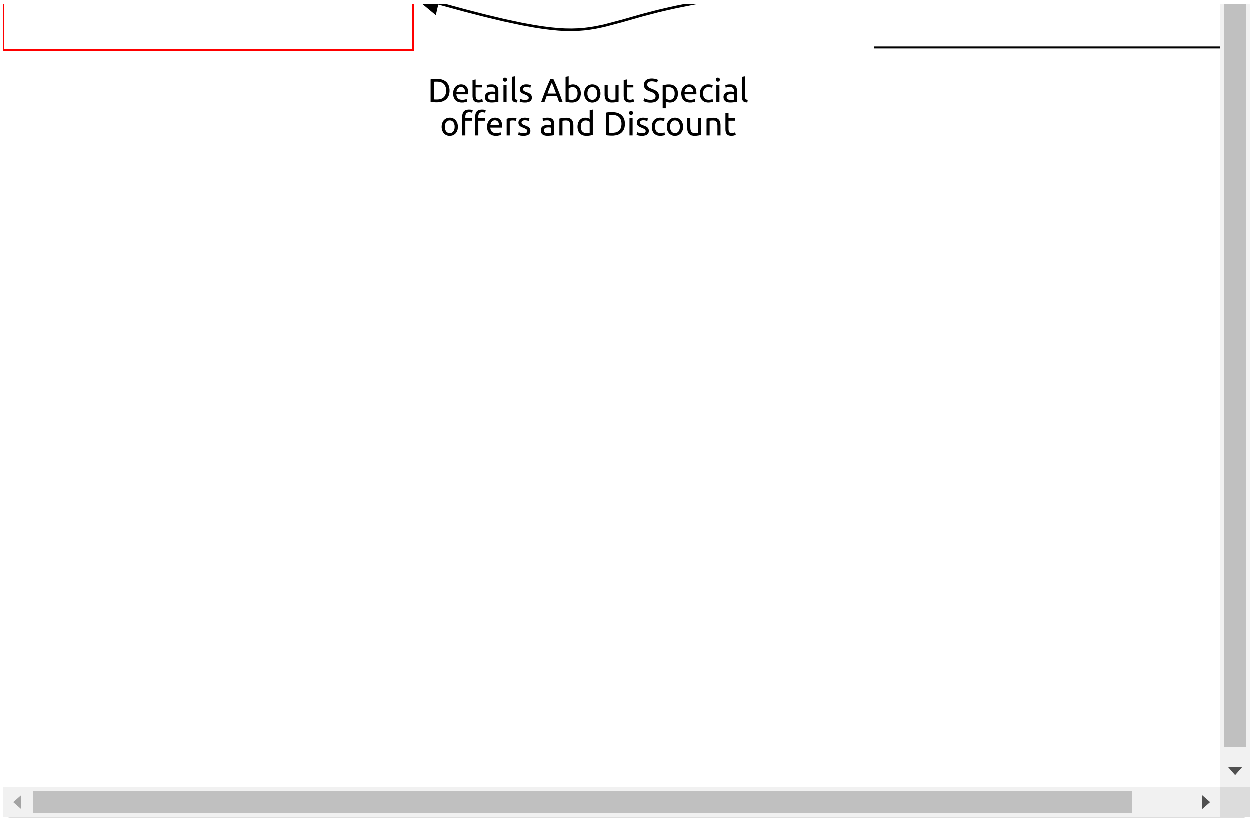
Returning the Result (Data Flow)

Description:

No threats listed.

Premium-User





Premium User (External Actor)

Description:

Premium User Privilage Escalation

Elevation of privilege, Open, Medium Severity

Description:
The normal user may able to view the offers and discounts that should be only accesible to the premium paid User

Mitigation:
Use Strong User Authentication mechnism

Special Offers and Coupons (Data Store)

Description:

No threats listed.

Details About Special offers and Discount (Data Flow)

Description:

No threats listed.