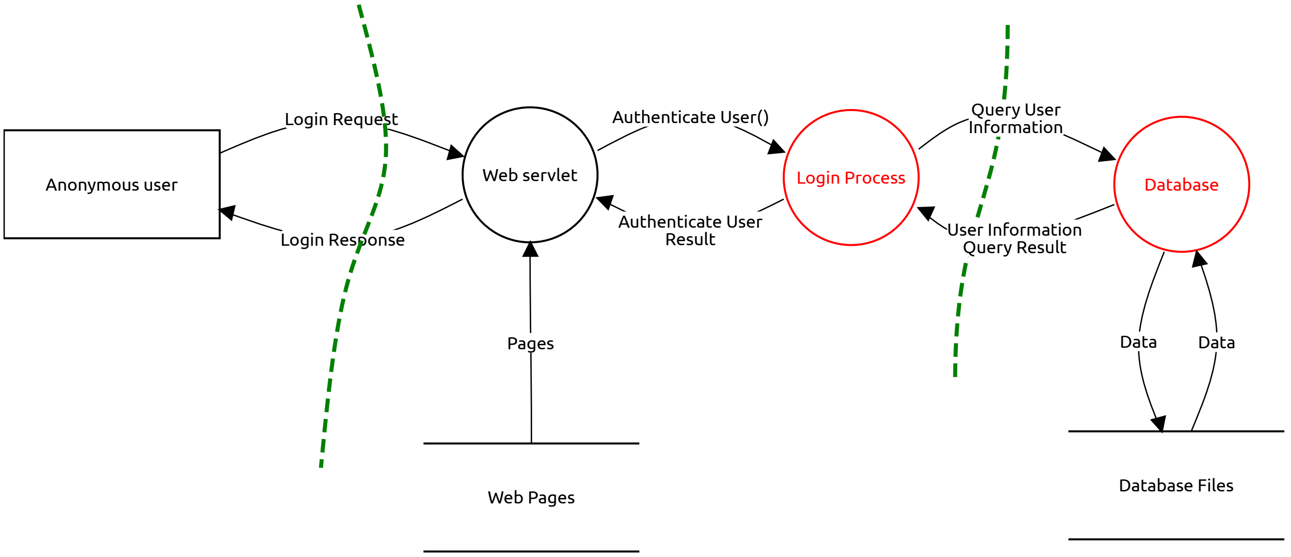
Threat model report for LezzetYolculuguThreatModels

Owner:
abderrahman fawzy
Reviewer:
Contributors:

High level system description

Login



Web servlet (Process)

No threats listed.

Anonymous user (External Actor)

No threats listed.

Login Request (Data Flow)

No threats listed.

Login Response (Data Flow)

No threats listed.

Login Process (Process)

Identity theft

Spoofing, Open, High Severity

Description:
The login process checks the password given by the user to the one in the database without prior hashing.
Mitigation:
Hash the password given by the user instead of saving plain text password into the database

Web Pages (Data Store)

No threats listed.

Pages (Data Flow)

No threats listed.

Database Files (Data Store)

Unauthorized access

Elevation of privilege, Mitigated, Medium Severity

Description:
Unauthorized access to database records.
Mitigation:
A role based database access is implemented.

Database (Process)

Data theft

Information disclosure, Open, High Severity

Description:
User passwords are saved as plain text which highly increase the likelihood of credential theft. Furthermore SQL injection attack can be conducted against the database. This threat can lead to disastrous consequences such as the theft of all database records
Mitigation:
Password hashes should be saved instead of plain text. Prepared SQL statements or entity database context should be used.

Authenticate User() (Data Flow)

No threats listed.

Authenticate User Result (Data Flow)

No threats listed.

Query User Information (Data Flow)

No threats listed.

User Information Query Result (Data Flow)

No threats listed.

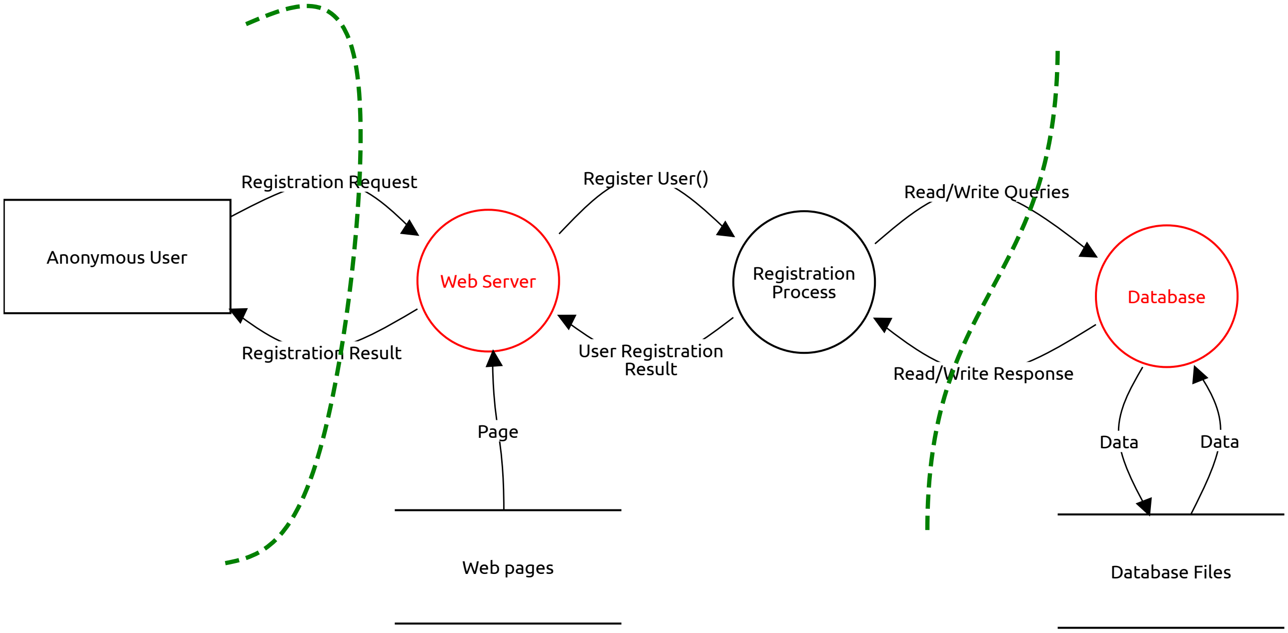
Data (Data Flow)

No threats listed.

Data (Data Flow)

No threats listed.

Sign up



Web Server (Process)

Data leakage

Information disclosure, Open, Medium Severity

Description:
Input received from users can be vector of cross site scripting, SQL injection and many more injection type attacks.
Mitigation:
Filter, escape, validate and encode user input

Registration Process (Process)

No threats listed.

Database (Process)

Data alteration

Tampering, Open, Medium Severity

Description:
SQL injection that can lead to alter or destroy data from the database
Mitigation:
SQL prepared statement or framework database context should be used

Malicious data insertion

Tampering, Open, Medium Severity

Description:
Harmful user input is potentially stored into the database for malicious intents
Mitigation:
Filter , validate and encode user input

Web pages (Data Store)

No threats listed.

Database Files (Data Store)

No threats listed.

Data (Data Flow)

No threats listed.

Data (Data Flow)

No threats listed.

Page (Data Flow)

No threats listed.

User Registration Result (Data Flow)

No threats listed.

Register User() (Data Flow)

No threats listed.

Read/Write Response (Data Flow)

No threats listed.

Anonymous User (External Actor)

No threats listed.

Registration Result (Data Flow)

No threats listed.

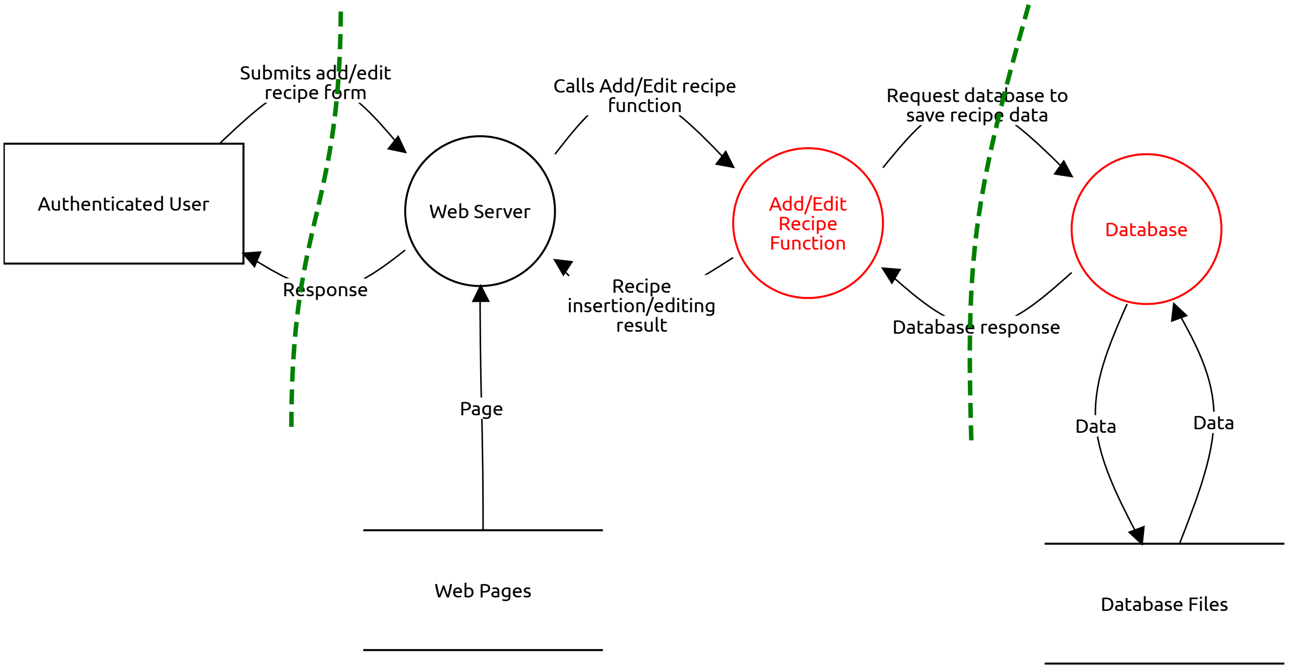
Registration Request (Data Flow)

No threats listed.

Read/Write Queries (Data Flow)

No threats listed.

Add recipe and edit recipe


Submits add/edit recipe form
Calls Add/Edit recipe function
Request database to save recipe data
Authenticated User
Web Server
Add/Edit Recipe Function
Database
Response
Recipe insertion/editing result
Database response
Page
Data
Data
Web Pages
Database Files

Authenticated User (External Actor)

No threats listed.

Web Server (Process)

No threats listed.

Add/Edit Recipe Function (Process)

Malicious user input storage

Tampering, Open, Medium Severity

Description:
Malicious user provided input can be stored that later on may prove to be harmful to the requesting users. Stored XSS is a potential danger.
Mitigation:
Filter, encode and validate user inputs

Database (Process)

Malicious user input storage

Tampering, Open, Medium Severity

Description:
Malicious user provided input can be stored that later on may prove to be harmful to the requesting users. Stored XSS is a potential danger.
Mitigation:
Filter, encode and validate user inputs

Web Pages (Data Store)

No threats listed.

Database Files (Data Store)

No threats listed.

Submits add/edit recipe form (Data Flow)

No threats listed.

Calls Add/Edit recipe function (Data Flow)

No threats listed.

Request database to save recipe data (Data Flow)

No threats listed.

Response (Data Flow)

No threats listed.

Recipe insertion/editing result (Data Flow)

No threats listed.

Database response (Data Flow)

No threats listed.

Page (Data Flow)

No threats listed.

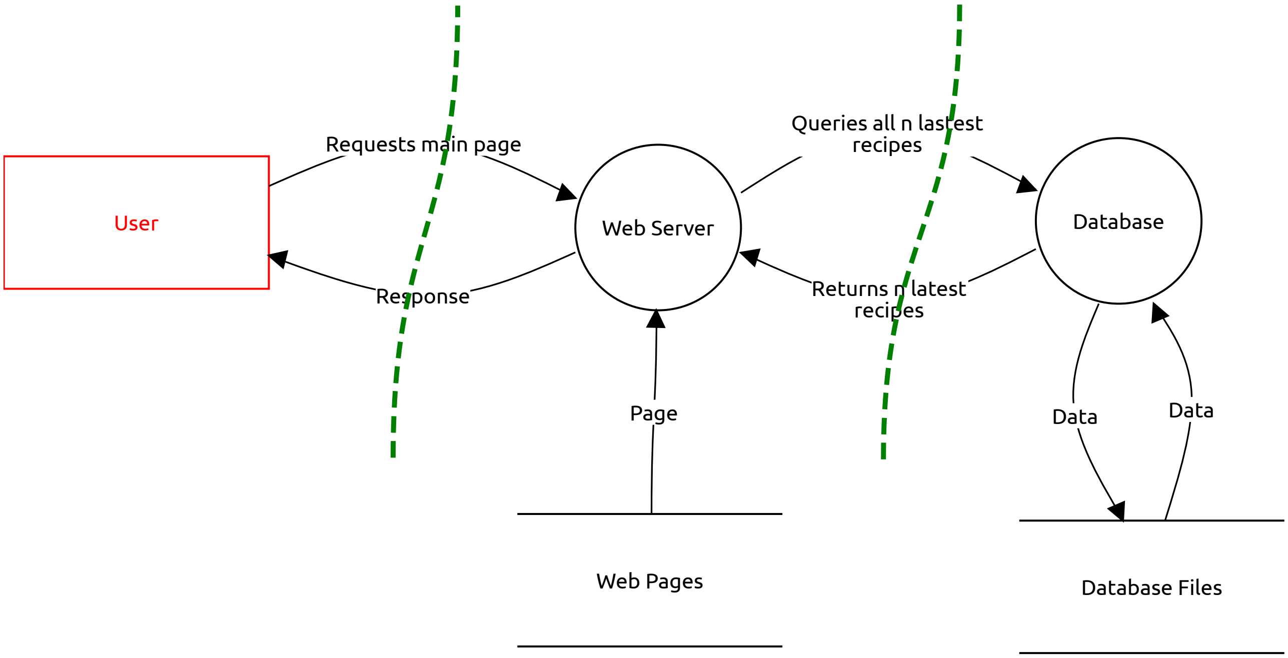
Data (Data Flow)

No threats listed.

Data (Data Flow)

No threats listed.

Main page



Web Server (Process)

No threats listed.

Database (Process)

No threats listed.

User (External Actor)

Browser data theft

Information disclosure, Open, Medium Severity

Description:
Data retrieved from the database is used in order to create the main page to send back to the user. In case malicious data is retrieved from the database and used to generate the main page, then the user is at a risk of having his/her data (browser side stored data such as cookies, sessions...) stolen
Mitigation:
Filter, escape and validate all user inputs

Web Pages (Data Store)

No threats listed.

Database Files (Data Store)

No threats listed.

Requests main page (Data Flow)

No threats listed.

Page (Data Flow)

No threats listed.

Data (Data Flow)

No threats listed.

Response (Data Flow)

No threats listed.

Data (Data Flow)

No threats listed.

Returns n latest recipes (Data Flow)

No threats listed.

Queries all n lastest recipes (Data Flow)

No threats listed.