Threat Model DESOFS

Proprietário: M1B_8
Revisor: FFS
Contribuidores: João Teixeira, Francisco Oliveira, Tomás Cancela
Data Gerada: Sat Apr 20 2024

Resumo Executivo

Descrição de alto nível do sistema (high level system)

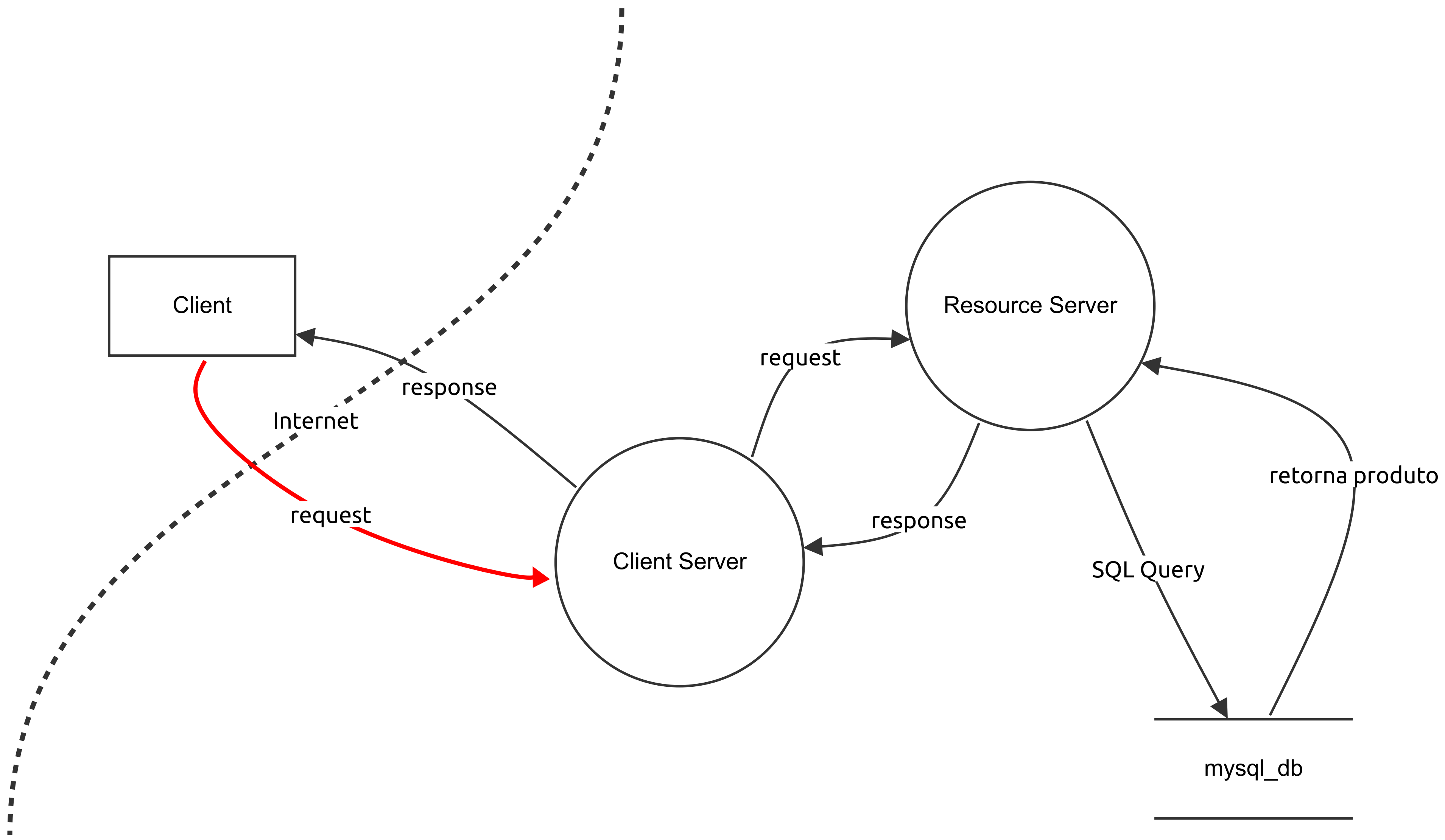
Product E-Commerce Website

Resumo

Ameaças totais	34
Total Mitigado	2
Não atenuado	32
Abrir / Alta Prioridade	19
Abrir / Prioridade Média	13
Abrir / Baixa Prioridade	0
Prioridade Aberta / Desconhecida	0

Add product to the shopping cart

As a Client, I want to add product to the shopping cart



Add product to the shopping cart

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Query (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

retorna produto (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

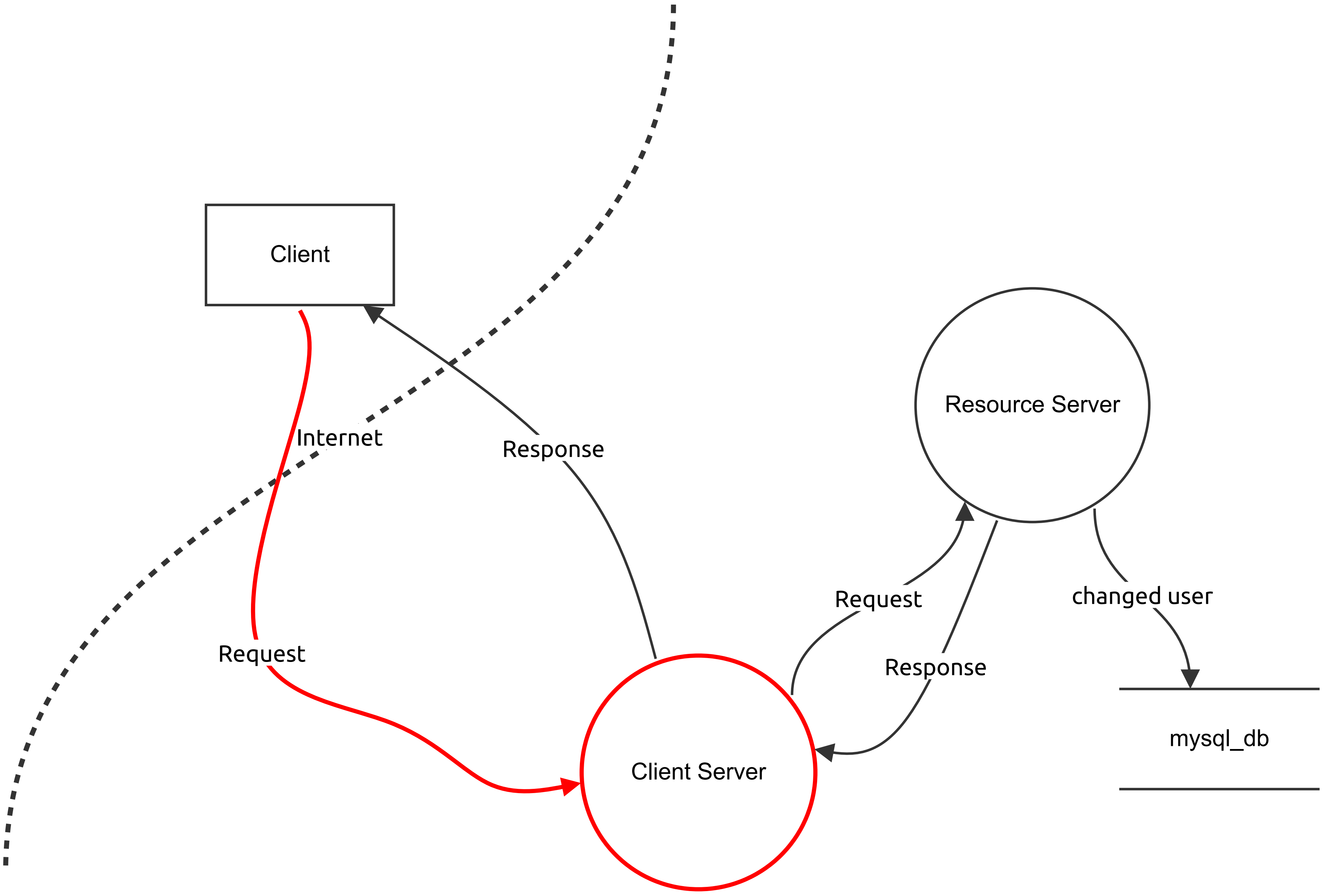
Number	Title	Type	Priority	Status	Score	Description	Mitigations
23	XSS (OWASP ID: A7:2017-Cross-Site Scripting (XSS))	Tampering	High	Open		Attackers inject malicious scripts into the product details or shopping cart pages, potentially stealing user information or executing unauthorized actions.	Implement input validation and output encoding, use Content Security Policy (CSP), sanitize user-generated content.
24	Insecure Direct Object References (IDOR) (OWASP ID: A4:2017-Insecure Direct Object References)	Tampering	High	Open		Attackers manipulate product identifiers or URLs to access other users' shopping cart items or product details.	Implement proper access controls and authorization checks, use indirect object references, validate user permissions.
25	Insecure Deserialization (OWASP ID: A8:2017-Insecure Deserialization)	Tampering	High	Open		Attackers exploit insecure deserialization to manipulate the data structure or execute arbitrary code when adding a product to the shopping cart.	Avoid using insecure deserialization, validate and sanitize serialized data, use strong data integrity checks.
26	Denial of Inventory (OWASP ID: A10:2017-Insufficient Logging & Monitoring)	Denial of service	High	Open		Attackers flood the system with requests to add products to the shopping cart, causing inventory depletion or service degradation.	Implement rate limiting, monitor inventory levels, use CDN (Content Delivery Network) or WAF (Web Application Firewall).
27	Broken Access Control (OWASP ID: A5:2017-Broken Access Control)	Tampering	Medium	Open		Lack of proper access controls might allow attackers to add products to the shopping cart without proper authorization.	Implement access controls and authorization checks, validate user permissions, use session management best practices.

Resource Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Change Password

As a Client, I want to change the password of my account



Change Password

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Resource Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	DDOS	Denial of service	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

changed user (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Fluxo de Dados)

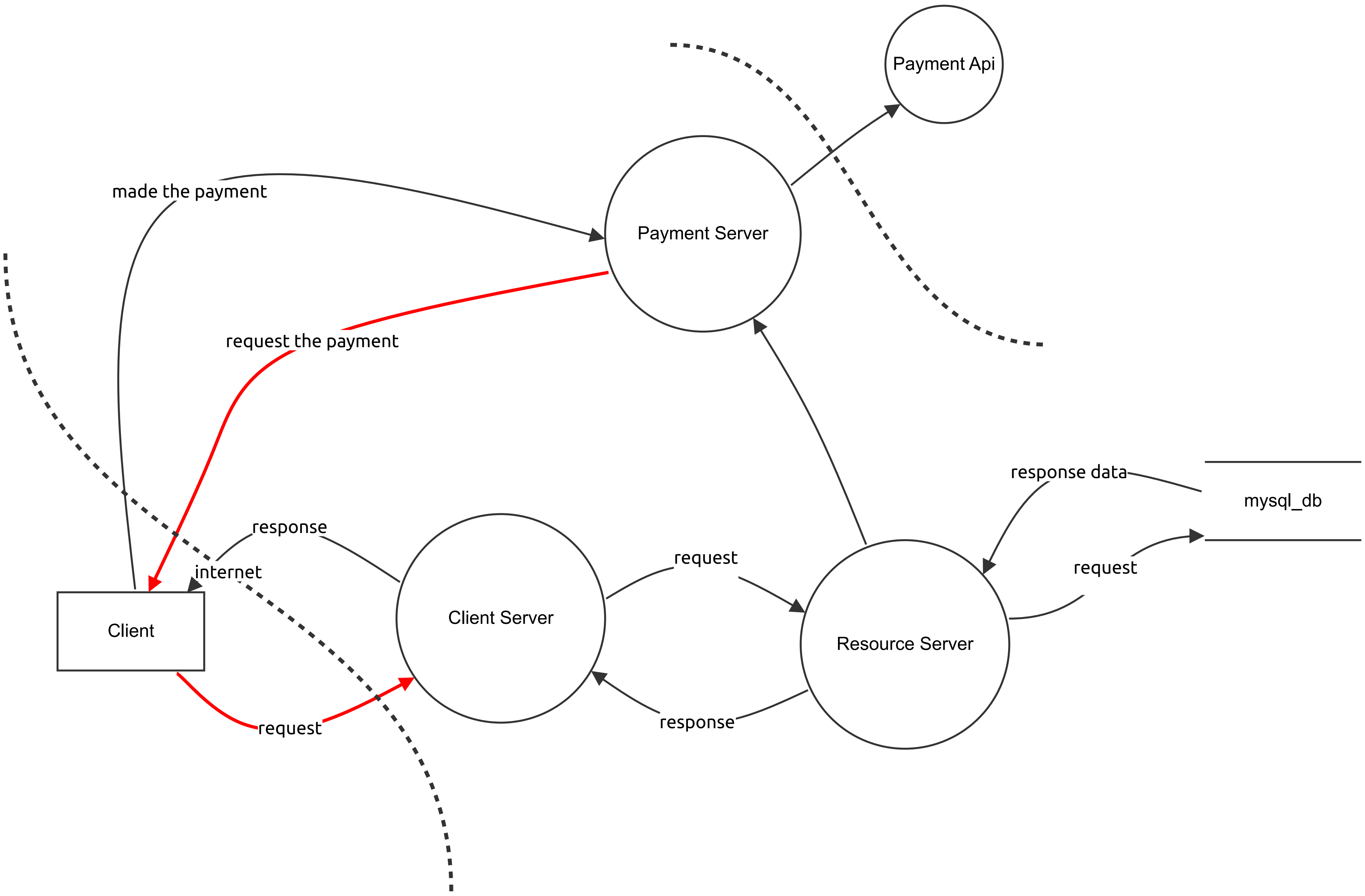
Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	XSS OWASP-ID-003	Tampering	High	Open		Injecting malicious scripts that could manipulate the password change process or steal new passwords.	Implement input validation, output encoding, and Content Security Policy (CSP).
13	Insecure Password Storage OWASP-ID-009	Information disclosure	Medium	Mitigated		New passwords stored in plaintext or weakly hashed form, making them susceptible to theft.	Use strong cryptographic hashing and salt passwords before storing them.
14	Insufficient Transport Layer Protection OWASP-ID-008	Tampering	High	Open		Lack of HTTPS or weak encryption could expose the new password during transmission.	Implement HTTPS with strong encryption, use HSTS (HTTP Strict Transport Security), and avoid mixed content.
15	Insecure Password Recovery OWASP-ID-010	Information disclosure	Medium	Open		Weak or easily guessable password recovery mechanisms that allow unauthorized password changes.	Implement secure password change processes with multi-factor authentication and security questions.
16	Insufficient Logging and Monitoring OWASP-ATC-004	Information disclosure	Medium	Open		Inability to detect and alert on suspicious password change attempts or patterns	Implement comprehensive logging, monitoring, and alerting mechanisms for password change events.

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Checkout the Shopping Cart

As a Client I want to checkout the Shopping Cart



Checkout the Shopping Cart

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Resource Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

made the payment (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request
(Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response data (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
28	(COUPON) XSS (OWASP ID: A7:2017-Cross-Site Scripting (XSS))	Tampering	Medium	Open		Attackers inject malicious scripts into the discount/coupon code input or display areas, potentially stealing user information or executing unauthorized actions.	Implement input validation and output encoding, use Content Security Policy (CSP), sanitize user-generated content.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
29	(COUPON) Insecure Direct Object References (OWASP ID: A4:2017-Insecure Direct Object References)	Tampering	High	Open		Attackers manipulate discount/coupon code identifiers or URLs to access or redeem other users' codes	Implement proper access controls and authorization checks, use indirect object references, validate user permissions
30	(COUPON) Insecure CAPTCHA Implementation (OWASP ID: A6:2017-Security Misconfiguration)	Tampering	Medium	Open		Weak or poorly implemented CAPTCHA can be bypassed by automated scripts or attackers during code redemption.	Use strong CAPTCHA mechanisms, regularly update and monitor CAPTCHA effectiveness, combine CAPTCHA with other anti-automation measures.
31	XSS (OWASP ID: A7:2017-Cross-Site Scripting (XSS))	Tampering	High	Open		Attackers inject malicious scripts into checkout pages or payment forms, potentially stealing user information or executing unauthorized actions.	Implement input validation and output encoding, use Content Security Policy (CSP), sanitize user-generated content.
32	Insecure Direct Object References (OWASP ID: A4:2017-Insecure Direct Object References)	Tampering	High	Open		Attackers manipulate order identifiers or URLs to access or modify other users' shopping carts or payment details.	Implement proper access controls and authorization checks, use indirect object references, validate user permissions.

request the payment (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
33	Insufficient Transport Layer Protection (OWASP ID: A6:2017-Security Misconfiguration)	Information disclosure	High	Open		Lack of HTTPS or weak encryption exposes payment and personal data during transmission.	Implement HTTPS with strong encryption, use HSTS (HTTP Strict Transport Security), avoid mixed content.
34	Payment Gateway Vulnerabilities (OWASP ID: A2:2017-Broken Authentication)	Tampering	High	Open		Vulnerabilities in payment gateway integration might allow attackers to manipulate payment data or bypass authentication.	Choose reputable payment gateways, follow secure integration practices, monitor for gateway-specific vulnerabilities and patches.
35	Fraudulent Transactions (OWASP ID: A9:2017-Using Components with Known Vulnerabilities)	Tampering	High	Open		Attackers exploit vulnerabilities to conduct fraudulent transactions or manipulate payment amounts.	Implement fraud detection mechanisms, monitor for suspicious activity, regularly update and patch payment systems and components.
37	Denial of Service (OWASP ID: A10:2017-Insufficient Logging & Monitoring)	Tampering	High	Open		Attackers flood the payment system with transaction requests, causing service degradation or denial of service.	Implement rate limiting, use CDN (Content Delivery Network) or WAF (Web Application Firewall), monitor server performance and network traffic.

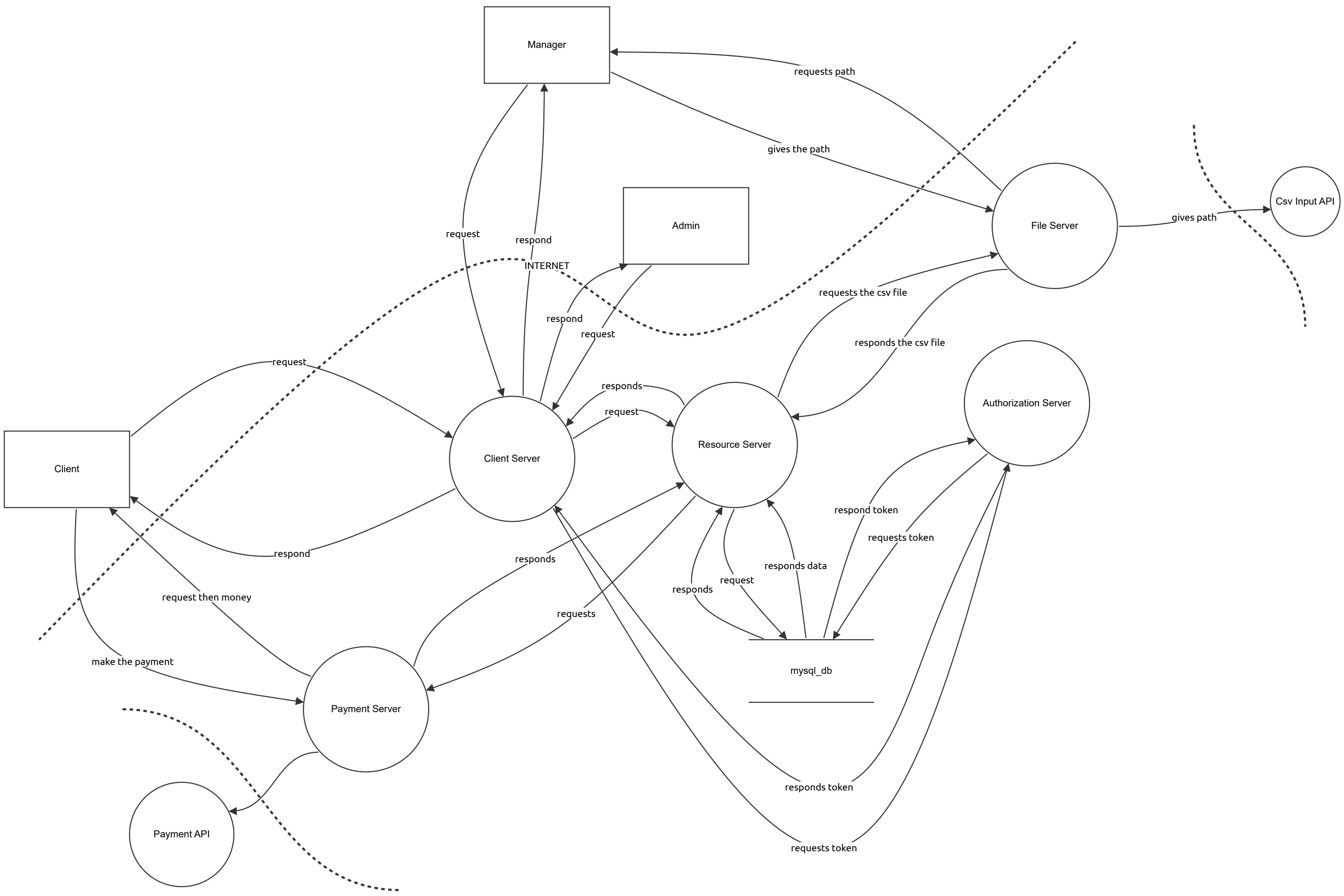
Payment Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment Api (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DFD


Manager
requests path
gives the path
request
respond
Admin
INTERNET
respond
request
File Server
gives path
Csv Input API
requests the csv file
responds the csv file
Authorization Server
request
responds
request
Client
Client Server
Resource Server
respond token
requests token
respond
request then money
responds
requests
responds data
request
responds
mysql_db
make the payment
Payment Server
Payment API
responds token
requests token

DFD

Client Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manager (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Admin (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

respond (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

respond (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

respond (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

make the payment (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request then money (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds data (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

requests (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

requests token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

requests token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

respond token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

gives the path (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

requests path (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

gives path (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

responds the csv file (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

requests the csv file (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Resource Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment API (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authorization Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

File Server (Processo)

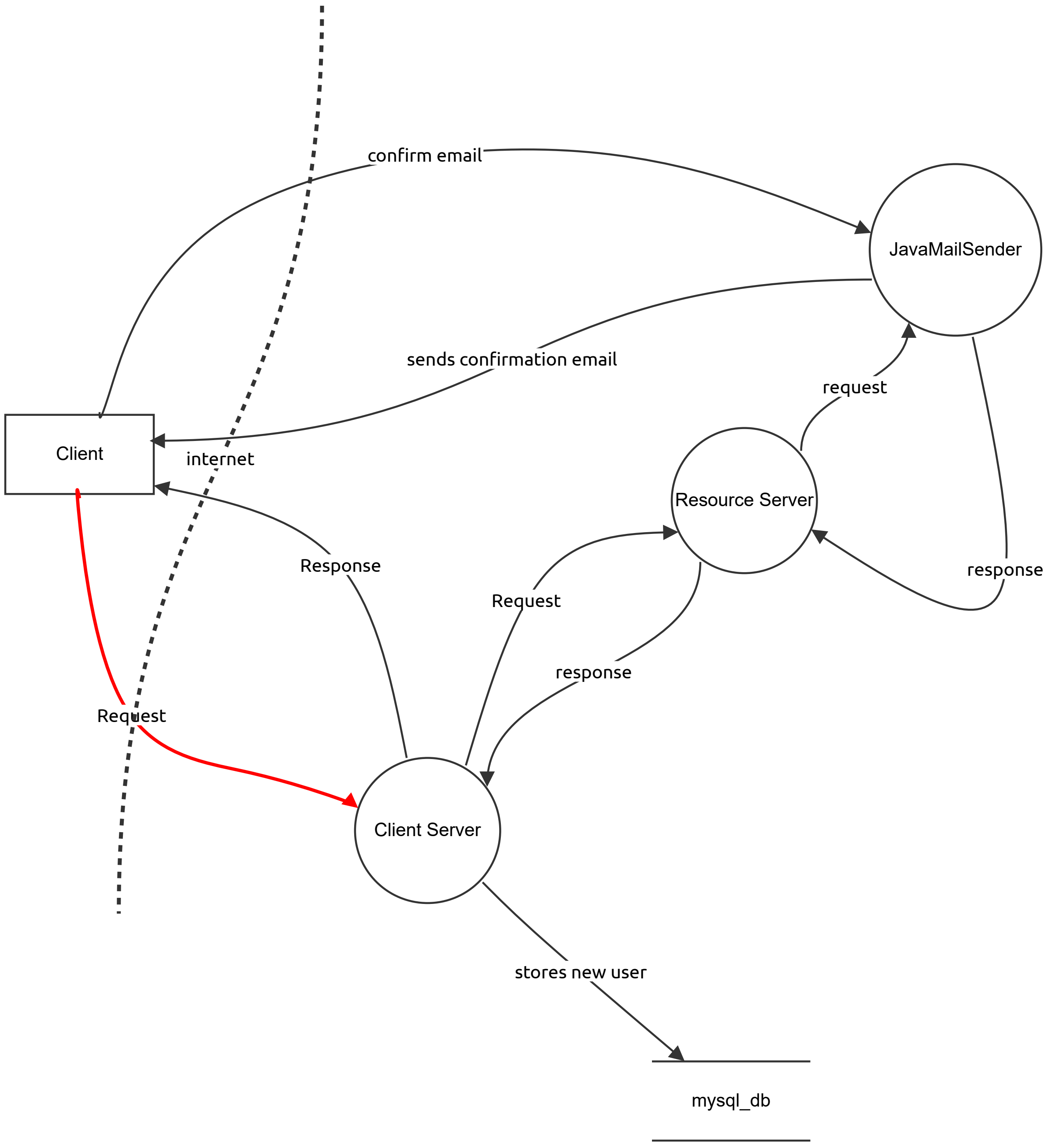
Number	Title	Type	Priority	Status	Score	Description	Mitigations

Csv Input API (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Register Account

I want to register a new account, using an email and password.



Register Account

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Resource Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client Server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

JavaMailSender (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

stores new user (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

confirm email (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

sends confirmation email (Fluxo de Dados)

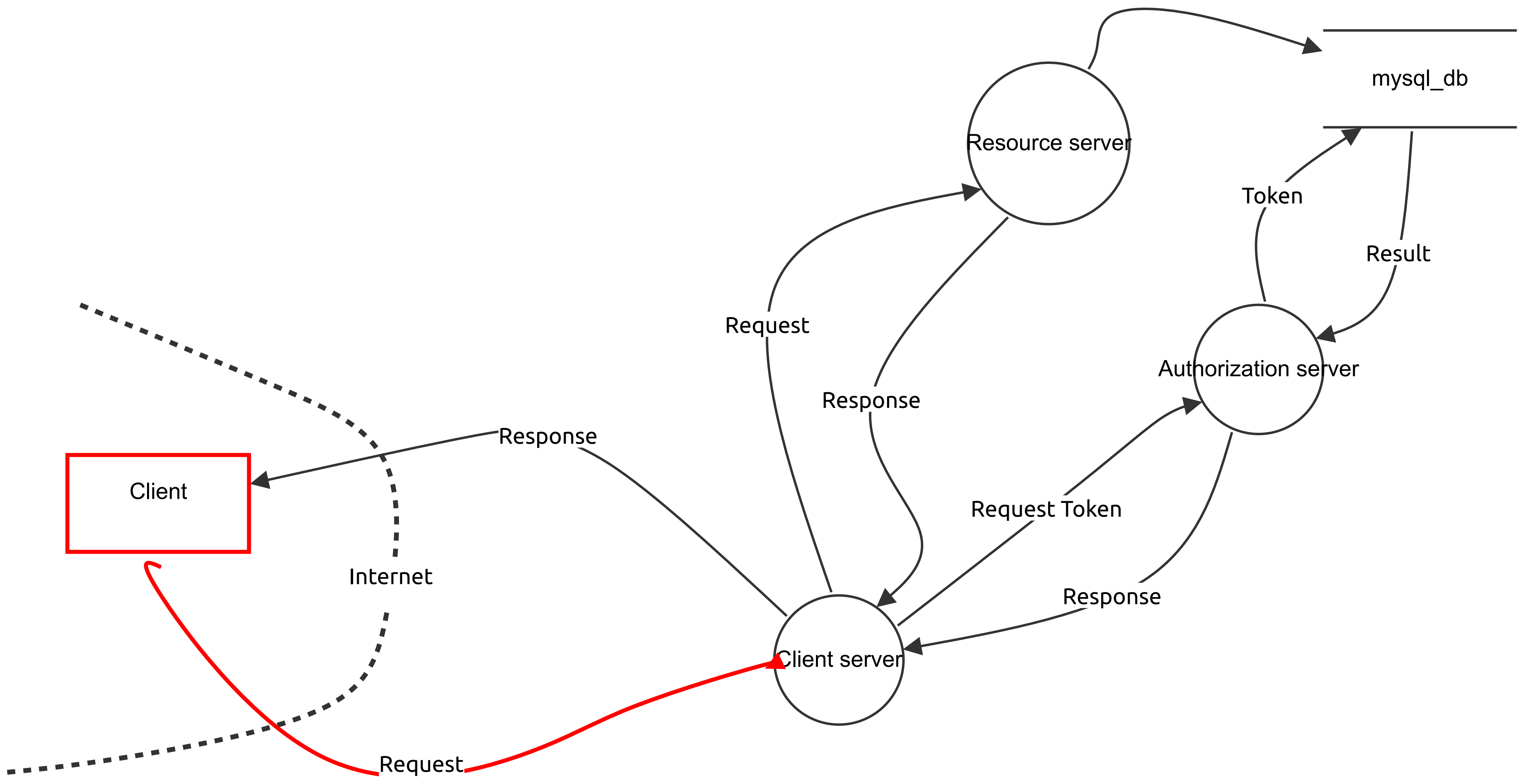
Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	Input Validation Bypass (OWASP ID: A7:2017-Cross-Site Scripting (XSS))	Tampering	Medium	Open		Provide a description for this threat	Implement server-side input validation, use secure coding practices, encode output
19	DOS (OWASP ID: A10:2017-Insufficient Logging & Monitoring)	Denial of service	High	Open		Attackers flood the registration system with a large volume of registration requests, causing service degradation or denial of service.	Implement rate limiting, use CDN (Content Delivery Network) or WAF (Web Application Firewall), monitor server performance and network traffic.
20	SQL Injection (OWASP ID: A1:2017-Injection)	Tampering	High	Open		Attackers inject SQL commands into the registration form's input fields, attempting to manipulate or compromise the database.	Use parameterized queries, implement input validation and sanitization, regularly update and patch software.
21	Insecure CAPTCHA Implementation (OWASP ID: A6:2017-Security Misconfiguration)	Tampering	Medium	Open		Weak or poorly implemented CAPTCHA can be bypassed by automated scripts or attackers.	Use strong CAPTCHA mechanisms, regularly update and monitor CAPTCHA effectiveness, combine CAPTCHA with other anti-automation measures.
22	Insufficient Anti-Automation (OWASP ID: A1:2017-Injection)	Tampering	Medium	Open		Attackers use automated tools or scripts to submit a large volume of fraudulent registrations.	Implement CAPTCHA, rate limiting, and behavioral analysis to detect and block automated registration attempts.

Sign In

As a Client, I want to sign in



Sign In

mysql_db (Armazenamento)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Resource server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authorization server (Processo)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Client (Ator)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Nova ameaça STRIDE	Spoofing	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Request (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Token (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Result (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response (Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request
(Fluxo de Dados)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	XSS OWASP-ID-003	Tampering	High	Open		Injecting malicious scripts into the sign-in page that could steal user credentials or perform actions on behalf of the user.	Implement input validation, output encoding, and Content Security Policy (CSP)
4	Brute Force Attack	Tampering	High	Open		Threat actors might attempt to guess or brute force credentials to gain unauthorized access.	Use CAPTCHA or multi-factor authentication (MFA) to prevent automated brute force attacks.
5	Credential Stuffing	Tampering	Medium	Open		Attackers use previously leaked credentials from other services to gain unauthorized access.	Monitor for unusual login patterns and implement MFA.
6	Man-in-the-Middle (MitM) Attack	Tampering	High	Open		An attacker intercepts communication between the client and server to capture login credentials.	Implement HTTPS with strong encryption.
7	Insecure Password Storage OWASP-ID-009	Information disclosure	Medium	Mitigated		Passwords stored in plaintext or weakly hashed form, making them susceptible to theft.	Hash passwords using strong cryptographic algorithms (e.g., bcrypt, Argon2). Use salts and implement password stretching.
8	Inadequate Account Lockout OWASP-ATC-003	Denial of service	Medium	Open		Lack of or ineffective account lockout mechanism could allow brute force attacks to continue without detection	Implement account lockout after a specified number of failed attempts and provide recovery options for legitimate users.
9	Insider Threats OWASP-ATC-005	Tampering	High	Open		Malicious insiders with access to the system might misuse their privileges to compromise user accounts.	Implement least privilege access controls, monitor insider activities, and conduct regular security awareness training.
10	Account Enumeration OWASP-ID-011	Information disclosure	Medium	Open		OWASP-ID-011	Implement generic error messages, use rate limiting on login attempts, and avoid revealing user-specific information.