securePro

Owner: G-03
Reviewer: Mamoona and Touseef
Contributors:
Date Generated: Mon Oct 14 2024

Executive Summary

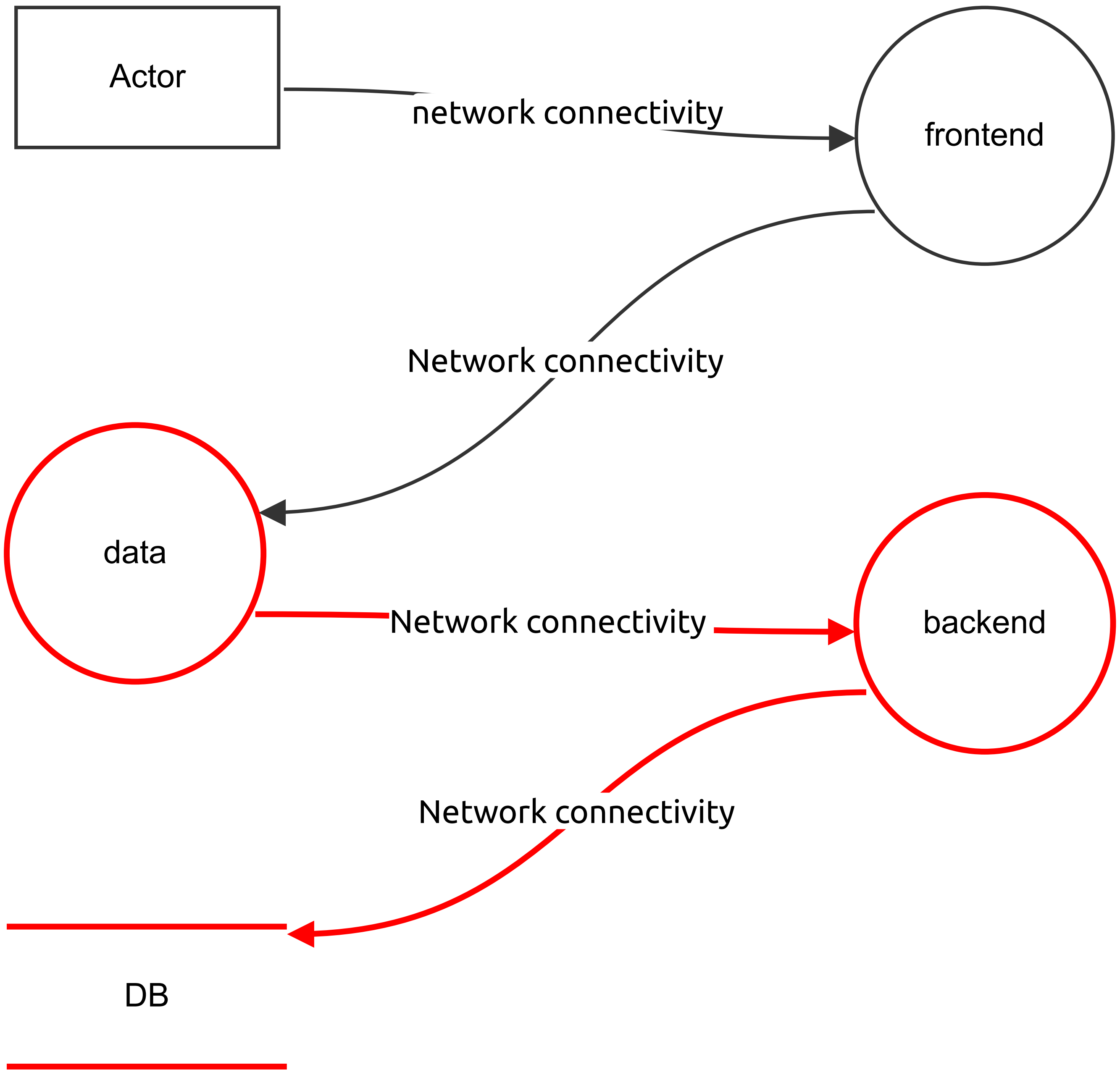
High level system description

Not provided

Summary

Total Threats	22
Total Mitigated	0
Not Mitigated	22
Open / High Priority	0
Open / Medium Priority	22
Open / Low Priority	0
Open / Unknown Priority	0

securePro


Actor
network connectivity
frontend
Network connectivity
data
Network connectivity
backend
Network connectivity
DB

securePro

Actor (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

frontend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Spoofing threat	Spoofing	Medium	Open		Unauthorized users impersonate legitimate data sources.	Implement strong data authentication (e.g., digital signatures).
7	Tempering threat	Tampering	Medium	Open		Unauthorized modification of data.	Use encryption and checksums; regularly audit data for changes.
8	Repudiation threat	Repudiation	Medium	Open		Users deny actions taken on data, creating disputes.	Maintain comprehensive logs of access and modifications.
9	Info Disclosure threat	Information disclosure	Medium	Open		Sensitive data is accessed by unauthorized users.	Encrypt sensitive data at rest and in transit; enforce strict access controls.
10	DOS threat	Denial of service	Medium	Open		Disruption in data availability due to overwhelming requests.	Implement rate limiting and redundancy in data storage.
11	Elevation of Privilege threat	Elevation of privilege	Medium	Open		Unauthorized users gain higher-level access to modify or view data.	Enforce role-based access control (RBAC) and limit permissions.

backend (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Spoofing threat	Spoofing	Medium	Open		Unauthorized users access backend services.	Implement strong authentication and session management.
15	Tampering threat	Tampering	Medium	Open		Code or configuration changes without authorization.	Regular code reviews and integrity monitoring.
16	Repudiation threat	Repudiation	Medium	Open		Users deny actions taken by backend services.	Maintain detailed logs of backend actions.
17	Info Disclosure threat	Information disclosure	Medium	Open		Sensitive data is exposed through backend vulnerabilities.	Apply the principle of least privilege and encrypt sensitive data.
18	DOS threat	Denial of service	Medium	Open		Backend services become overwhelmed and unavailable.	Use load balancing and distributed architectures.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
19	Elevation of Privilege threat	Elevation of privilege	Medium	Open		Unauthorized escalation of privileges within backend processes.	Regularly review permissions and enforce least privilege.

DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Tampering threat	Tampering	Medium	Open		Unauthorized modification of database records.	Use integrity checks and maintain logs of all transactions.
22	Repudiation threat	Repudiation	Medium	Open		Users deny database actions taken, creating accountability issues.	Keep detailed access logs for all database interactions.
23	Info Disclosure threat	Information disclosure	Medium	Open		Sensitive information is exposed to unauthorized users.	Encrypt sensitive data and enforce strict access controls.
24	Dos threat	Denial of service	Medium	Open		Database services are rendered unavailable due to excessive requests.	Implement connection pooling and throttling.

network connectivity (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Network connectivity (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Network connectivity (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Tampering threat	Tampering	Medium	Open		Data packets are altered during transmission.	Use hashing and digital signatures on data packets.
12	Info Disclosure threat	Information disclosure	Medium	Open		Sensitive information is intercepted during data transfer.	Encrypt data flows and use secure channels.
13	DOS threat	Denial of service	Medium	Open		High data flow volume disrupts service.	Implement throttling and load balancing.

Network connectivity (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Tampering threat	Tampering	Medium	Open		Data packets are altered during transmission.	Use hashing and digital signatures on data packets.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Info Disclosure threat	Information disclosure	Medium	Open		Sensitive information is intercepted during data transfer.	Encrypt data flows and use secure channels.
21	Dos STRIDE	Denial of service	Medium	Open		High data flow volume disrupts service.	Implement throttling and load balancing.