Damanitech Threat Model

Owner: Dada Ojuko
Reviewer: Mr. Ali
Contributors:
Date Generated: Sat Nov 29 2025

Executive Summary

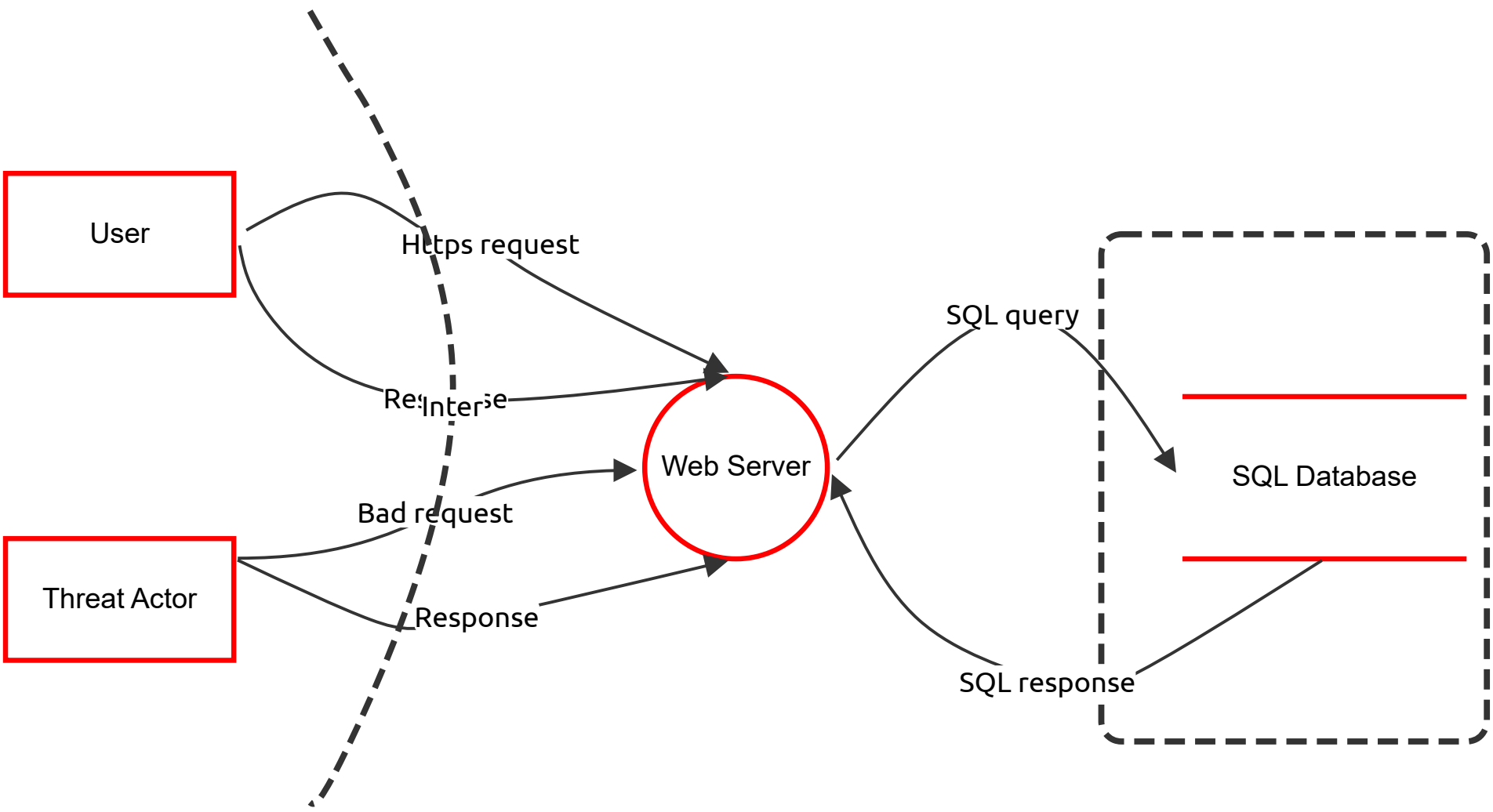
High level system description

Not provided

Summary

Total Threats	15
Total Mitigated	0
Total Open	15
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	15

Damanitech Web App DFD



Damanitech Web App DFD

SQL Database (Store)

Description: Storage for everything

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	SQL threat	Tampering	TBD	Open		The stored documents integrity could be compromised	Data Encryption
2	New STRIDE threat	Repudiation	TBD	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
3	SQL threat	Tampering	TBD	Open		The stored documents integrity could be compromised	Data Encryption
4	SQL threat	Repudiation	TBD	Open		Action not performed by user	A trail system has to be implemented to manage logs
5	SQL threat	Information disclosure	TBD	Open		Unauthorized access to confidential data	MFA (Multi Factor authentication)
6	SQL threat	Denial of service	TBD	Open		Authorized user data compromised availability	Rate limiting by employing anti-DOS software

Web Server (Process)

Description: The web server

Number	Title	Type	Severity	Status	Score	Description	Mitigations
7	Web Server threat	Spoofing	TBD	Open		Users can be impersonated.	Professional and customized domain usage.
8	Web Server threat	Tampering	TBD	Open		Unauthorized modification of data, code, configurations, or communications. Affects integrity and can alter system behaviour.	Hashing, digital signatures, TLS, RBAC, input validation, file integrity monitoring, config hardening, WAF, change control processes, secure logging.
9	Web Server threat	Repudiation	TBD	Open		Attackers perform malicious activity and deny it because there is no reliable logging or audit trail.	Detailed access and action logs, Use unique user accounts (no shared admin accounts).
10	Web Server threat	Information disclosure	TBD	Open		Sensitive data is exposed via the web server or its components.	Strict access controls on storage buckets, Input/output data filtering, Disable verbose error messages in production and Encrypt data at rest and in transit.
11	Web Server threat	Denial of service	TBD	Open		Attacker overwhelms or exhausts the web server's resources, making it unavailable to legitimate users.	Web application firewall (WAF), CDN protection (Cloudflare) and Health checks.
12	Web Server threat	Elevation of privilege	TBD	Open		Attacker gains higher privileges on the web server or backend system.	Least privilege access (RBAC), Harden server OS (disable unused services), Patch management / automatic updates, Disable remote root login.

User (Actor)

Description: Normal user authenticated/unauthenticated

Number	Title	Type	Severity	Status	Score	Description	Mitigations
13	User threat	Spoofing	TBD	Open		Attacker impersonates a user	MFA, secure sessions, adaptive auth, phishing prevention.
14	User threat	Repudiation	TBD	Open		User denies performing actions	Tamper-proof logs, digital signatures, strong audit trails

Threat Actor (Actor)

Description: Bad user authenticated/unauthenticated

Number	Title	Type	Severity	Status	Score	Description	Mitigations
15	Threat Actor	Spoofing	TBD	Open		Impersonates identities or systems.	MFA, Zero Trust, signed tokens.

Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Bad request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SQL query (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SQL response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Https request (Data Flow)

Description: Normal https request

Number	Title	Type	Severity	Status	Score	Description	Mitigations