WebApp Threat Model

Owner: ming_21920794
Reviewer:
Contributors:
Date Generated: Wed Oct 29 2025

OWASP Threat Dragon

Executive Summary

High level system description

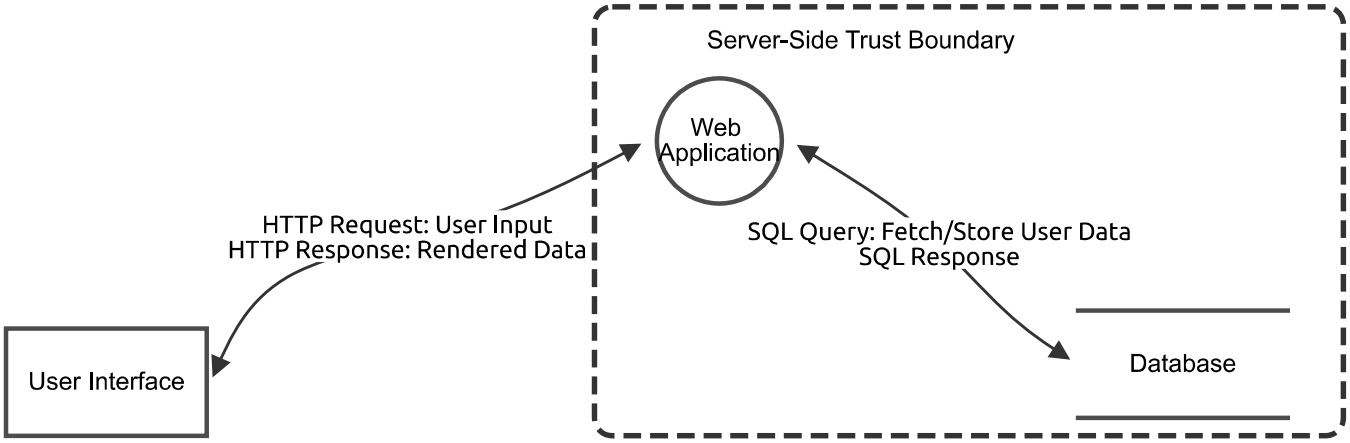
Not provided

Summary

Total Threats	18
Total Mitigated	0
Total Open	18
Open / Critical Severity	4
Open / High Severity	6
Open / Medium Severity	6
Open / Low Severity	2

WebApp DFD

21920794



WebApp DFD

User Interface (Actor)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
2	[S] UI Spoofing - Session Hijack		Critical	Open		Attacker steals cookies to impersonate user.	HttpOnly + Secure + SameSite cookies, JWT.
3	[T] UI Tampering - XSS Injection		High	Open		Malicious script alters form input.	CSP, input sanitization, output encoding.
4	[R] UI Repudiation - No Action Proof		Low	Open		User denies submitting data.	Client-side signed timestamps.
5	[I] UI Info Disclosure - Error Leaks		Medium	Open		Verbose errors expose system info.	Generic error messages.
6	[D] UI DoS - JS Flood		Medium	Open		Malformed input freezes browser.	Rate limiting, JS sandbox.
7	[E] UI EoP - DOM Bypass		Medium	Open		Client-side logic trusts manipulated DOM.	Server-side authorization only.

Web Application (Process)

Properties: Web Application

Number	Title	Type	Severity	Status	Score	Description	Mitigations
8	[S] App Spoofing - MITM on HTTPS	Spoofing	High	Open		Intercepts traffic over public network.	TLS 1.3, HSTS, cert pinning.
9	[T] App Tampering - SQL Injection	Tampering	Critical	Open		Input modifies DB queries.	Parameterized queries, ORM.
10	[R] App Repudiation - No Logs	Repudiation	Medium	Open		Actions not traceable.	Immutable audit logs.
11	[I] App Info Disclosure - Data Leak	Information disclosure	High	Open		PII sent unencrypted.	Encrypt in transit/rest.
12	[D] App DoS - Resource Exhaustion	Denial of service	Medium	Open		High load crashes server.	Auto-scaling, timeouts.
13	[E] App EoP - Broken ACL	Elevation of privilege	High	Open		Unauthorized endpoint access.	RBAC, least privilege.

Database (Store)

Properties: Encrypted, Stores Credentials

Number	Title	Type	Severity	Status	Score	Description	Mitigations
14	[S] DB Spoofing - Credential Theft	Information disclosure	High	Open		Stolen DB login.	MFA, IP whitelist.
15	[T] DB Tampering - Row Edit	Tampering	Critical	Open		Direct data change.	Row-level security.

Number	Title	Type	Severity	Status	Score	Description	Mitigations
16	[R] DB Repudiation - No Audit	Repudiation	Low	Open		No change trail.	Immutable audit.
17	[I] DB Info Disclosure - Plaintext	Information disclosure	High	Open		Data at rest exposed.	TDE encryption.
18	[D] DB DoS - Connection Flood	Denial of service	Medium	Open		Too many connections.	Pooling, limits.
19	[E] DB EoP - SQL Escalation	Elevation of privilege	Critical	Open		Read → admin via injection.	Stored procedures.

HTTP Request: User Input HTTP Response: Rendered Data (Data Flow)

Properties: Encrypted, Protocol (HTTPS)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SQL Query: Fetch/Store User Data SQL Response (Data Flow)

Properties: Encrypted, Protocol (SQL)

Number	Title	Type	Severity	Status	Score	Description	Mitigations