SpendSmart

Owner: Liam Dodd
Reviewer:
Contributors:
Date Generated: Sun Mar 10 2024

Executive Summary

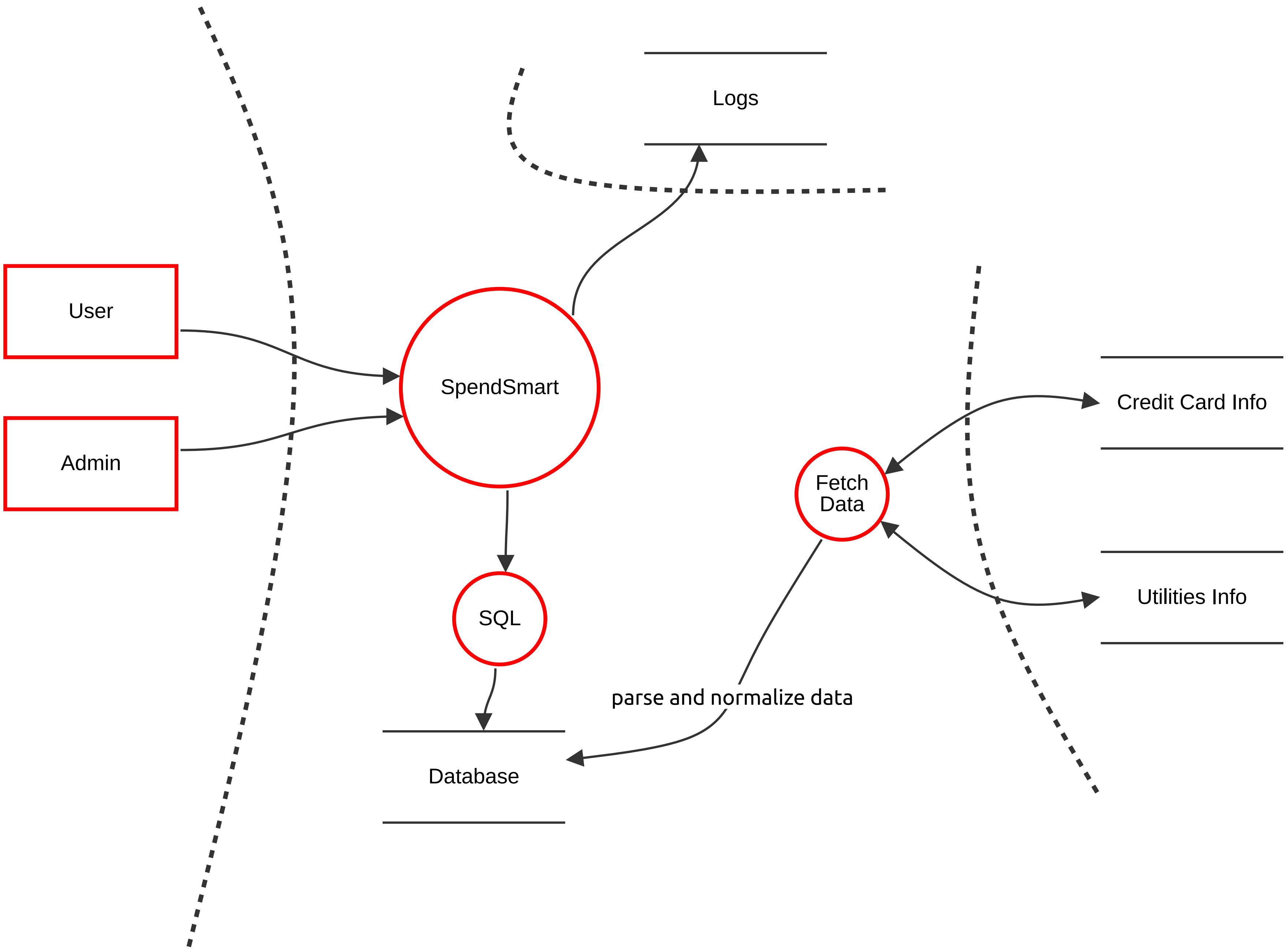
High level system description

SpendSmart is a digital budgeting app that integrates personal financial information from various sources to provide a seamless and secure way to manage finances. It utilizes encryption for sensitive data at rest and in transit. Multi-factor authentication is used for user and admin access. Logging is encrypted and access is restricted.

Summary

Total Threats	12
Total Mitigated	4
Not Mitigated	8
Open / High Priority	4
Open / Medium Priority	4
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

Credit Card Info (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilities Info (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Fetch Data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	AtiM PtC	Spoofing	Medium	Open	7	attackers could target the token based authentication to perform Attacker-in-the-Middle (AitM) and Pass-the-Cookie (PtC) attacks	restrict access to tokens and limit access to known devices

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

parse and normalize data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	New STRIDE threat	Denial of service	Medium	Mitigated		potential for regex exploitation	ensure parsing algorithm is hardened against evil regex

SpendSmart (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Code injection	Denial of service	Medium	Open	7	Code injection	Sanitize user inputs
10	XSS	Denial of service	High	Open	8	cross site scripting attacks	utilize security headers to mitigate scripting attacks
15	Privilage	Elevation of privilege	High	Open	8	Attacker could utilize vulnerabilities, misconfiguration, malware, or social engineering to modify privileges and gain full access to the system	Enforce least privilege and monitor privileged sessions

Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Key Management	Information disclosure	Medium	Mitigated		Loss of confidentially if keys or encryption is not configured properly	Audit encryption and ensure keys are not accessible to attackers

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Phishing	Spoofing	Medium	Open	7	Phishing attack	educate users about the risk of phishing and push bombing attacks

Admin (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	RBAC	Spoofing	Medium	Open	7	Role Based Access Control misuse	permissions are clearly defined, documented and have a process for creating, modifying, and deleting roles and permissions
6	Phishing	Spoofing	High	Open	8	Phishing attack	Ensure users with admin access receive proper training against social engineering tactics and implement zero trust

SQL (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	SQL Injection	Information disclosure	High	Open	8	users could use SQL injection to bypass authentication or access sensitive information	input sanitation

Logs (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Change logs	Tampering	Medium	Mitigated		modify/change logs	ensure logs are encrypted and access restricted
14	Responsiblity	Repudiation	Medium	Mitigated		If attackers gain access to logs it would be difficult to assign responsibility	restrict access and encrypt