Luttrell_CSD370

Owner: Jason Luttrell
Reviewer: Vianelis Martinez
Contributors:
Date Generated: Sun Jun 15 2025

Executive Summary

High level system description

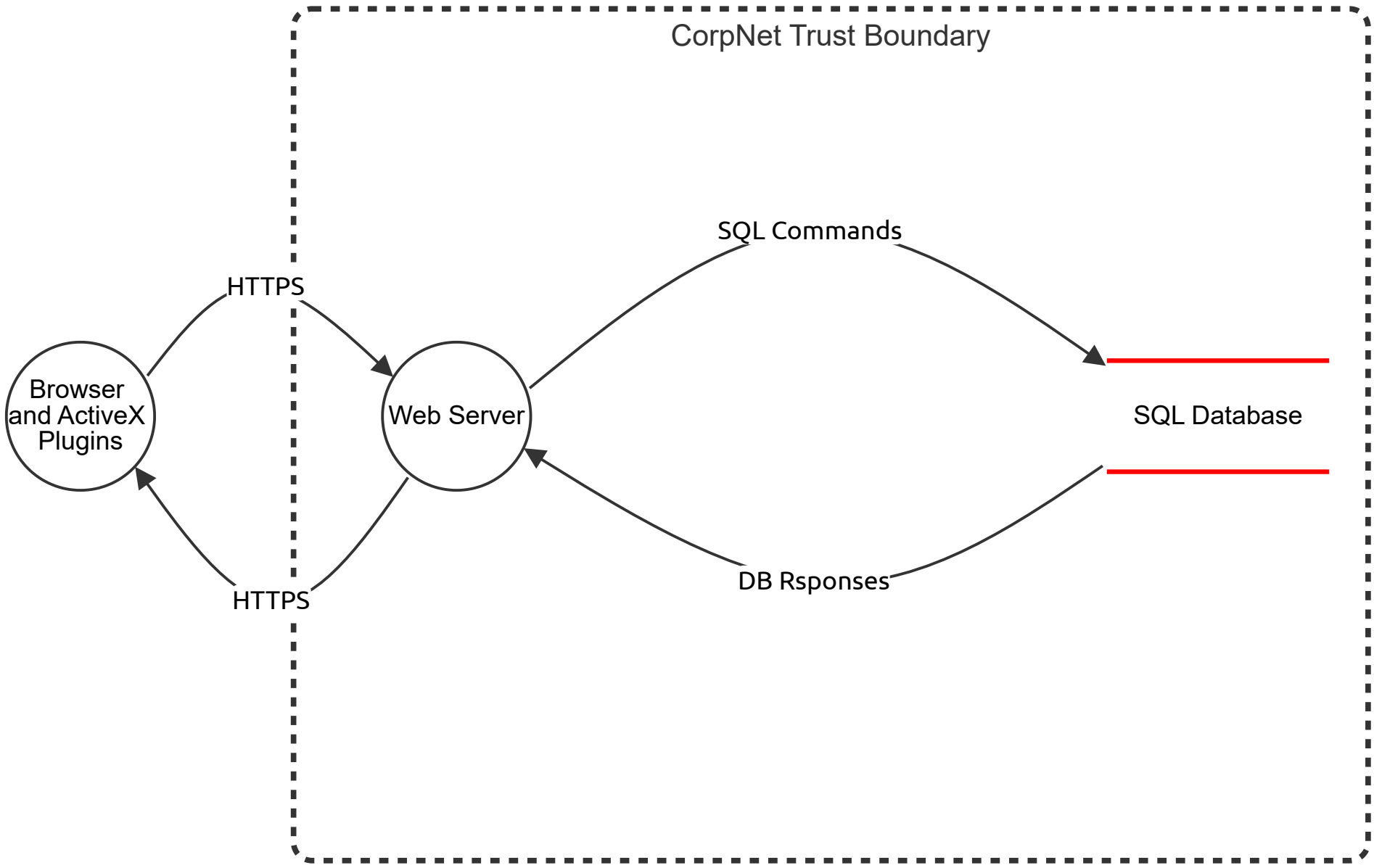
Not provided

Summary

Total Threats	3
Total Mitigated	1
Not Mitigated	2
Open / High Priority	1
Open / Medium Priority	0
Open / Low Priority	1
Open / Unknown Priority	0

CSD370

Module 3.2 assignment



CSD370

Browser and ActiveX Plugins (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	SQL DDoS Threat	Denial of service	Low	Open		A DDoS (Distributed Denial of Service) attack against a SQL database is a type of cyberattack in which multiple compromised systems (often part of a botnet) flood the database server with excessive, malicious traffic or requests, with the goal of making the service unavailable to legitimate users	Network-Level Mitigations: 1. Use a Web Application Firewall (WAF): Filters traffic before it hits the application layer. 2. Deploy a DDoS Protection Service: Cloud providers like AWS Shield, Azure DDoS Protection, and Cloudflare offer DDoS mitigation as a service. 3. Rate Limiting / Throttling: Limit the number of requests allowed from a single IP over a time window.
2	SQL Injection Attack	Information disclosure	Medium	Mitigated		An unauthorized information disclosure threat for a SQL database involves the exposure of sensitive data to individuals or systems not authorized to access it. This type of threat compromises confidentiality, one of the three pillars of the CIA Triad (Confidentiality, Integrity, Availability). SQL Injection Attacks: Attackers insert malicious SQL code into input fields to bypass authentication or extract data (e.g., SELECT * FROM users). Example: An attacker retrieves usernames, passwords, or payment information by manipulating a vulnerable login form.	Use parameterized queries to prevent SQL injection.
3	Misconfigured Access Controls	Tampering	High	Open		An unauthorized information disclosure threat for a SQL database involves the exposure of sensitive data to individuals or systems not authorized to access it. This type of threat compromises confidentiality, one of the three pillars of the CIA Triad (Confidentiality, Integrity, Availability). Misconfigured Access Controls: Users or applications have more permissions than necessary (e.g., read access to the entire database). Example: A front-end server account has access to sensitive tables it doesn't need (e.g., HR or financial records).	1. Implement least privilege access control (e.g., role-based permissions). 2. Audit access histories for users. 3. Audit roles periodically.

Web Server (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTPS (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTPS (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Commands (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

DB Rsponses (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations