Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Thu Oct 10 2024

Executive Summary

High level system description

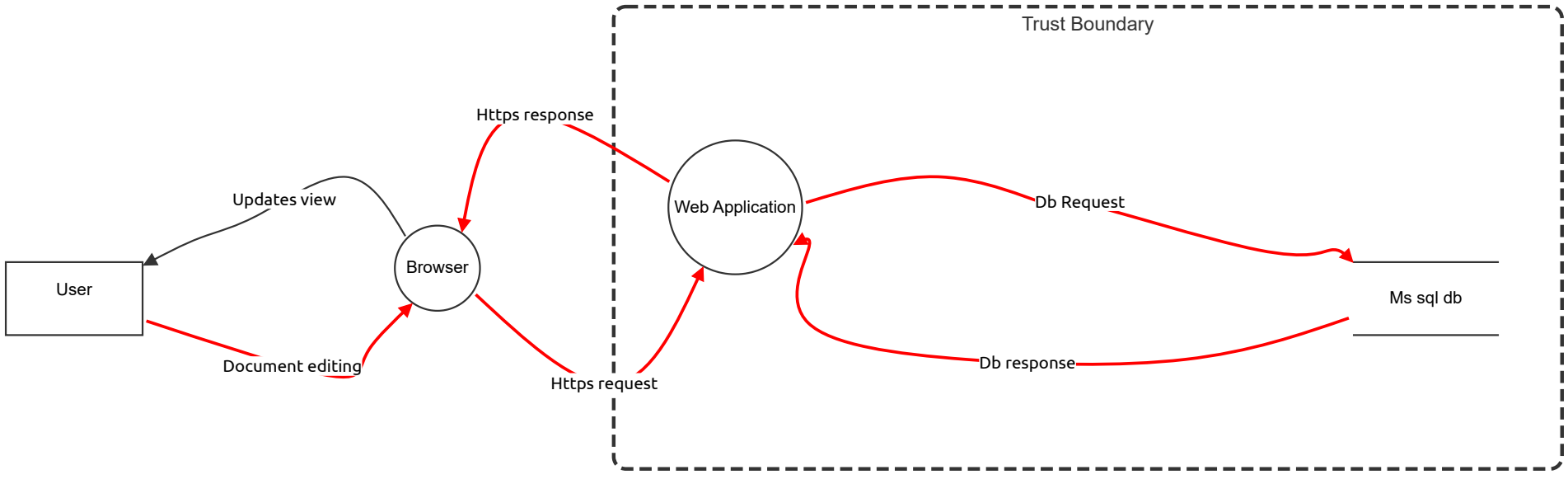
Not provided

Summary

Total Threats	16
Total Mitigated	0
Not Mitigated	16
Open / High Priority	2
Open / Medium Priority	14
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram

Jigsaw



New STRIDE diagram

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ms sql db (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web Application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Updates view (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Db Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Potential Excessive Resource Consumption for Web Server or SQL Database	Tampering	High	Open		Does Web Server or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job.	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Potential SQL Injection Vulnerability for SQL Database	Tampering	Medium	Open		SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities.	Provide remediation for this threat or a reason if status is N/A
1	Potential SQL Injection Vulnerability for SQL Database	Denial of service	High	Open		SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities.	Provide remediation for this threat or a reason if status is N/A

Db response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
4	Persistent Cross Site Scripting	Tampering	Medium	Open		The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SQL Database' inputs and output.	Provide remediation for this threat or a reason if status is N/A
4	Cross Site Scripting	Tampering	Medium	Open		The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	Provide remediation for this threat or a reason if status is N/A
4	Spoofing of Source Data Store SQL Database	Denial of service	Medium	Open		SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server. Consider using a standard authentication mechanism to identify the source data store.	Provide remediation for this threat or a reason if status is N/A

Https request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Spoofing the Browser Client Process	Denial of service	Medium	Open		Browser Client may be spoofed by an attacker and this may lead to unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the source process.	Provide remediation for this threat or a reason if status is N/A
8	Potential Data Repudiation by Web Server	Tampering	Medium	Open		Web Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Provide remediation for this threat or a reason if status is N/A
8	Potential Process Crash or Stop for Web Server	Denial of service	Medium	Open		Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Provide remediation for this threat or a reason if status is N/A
11	Data Flow HTTPS Request Is Potentially Interrupted	Denial of service	Medium	Open		An external agent interrupts data flowing across a trust boundary in either direction.	Provide remediation for this threat or a reason if status is N/A
11	Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Information disclosure	Medium	Open		Browser Client may be able to remotely execute code for Web Server.	Provide remediation for this threat or a reason if status is N/A

Https response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Web Server Process Memory Tampered	Tampering	Medium	Open		An external agent interrupts data flowing across a trust boundary in either direction.	Provide remediation for this threat or a reason if status is N/A

Document editing (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Spoofing the Human User External Entity	Tampering	Medium	Open		Human User may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify the external entity.	Provide remediation for this threat or a reason if status is N/A
11	Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Information disclosure	Medium	Open		Browser Client may be able to remotely execute code for Web Server.	Provide remediation for this threat or a reason if status is N/A
11	Elevation Using Impersonation	Information disclosure	Medium	Open		Browser Client may be able to impersonate the context of Human User in order to gain additional privilege.	Provide remediation for this threat or a reason if status is N/A