Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Sat Oct 26 2024

Executive Summary

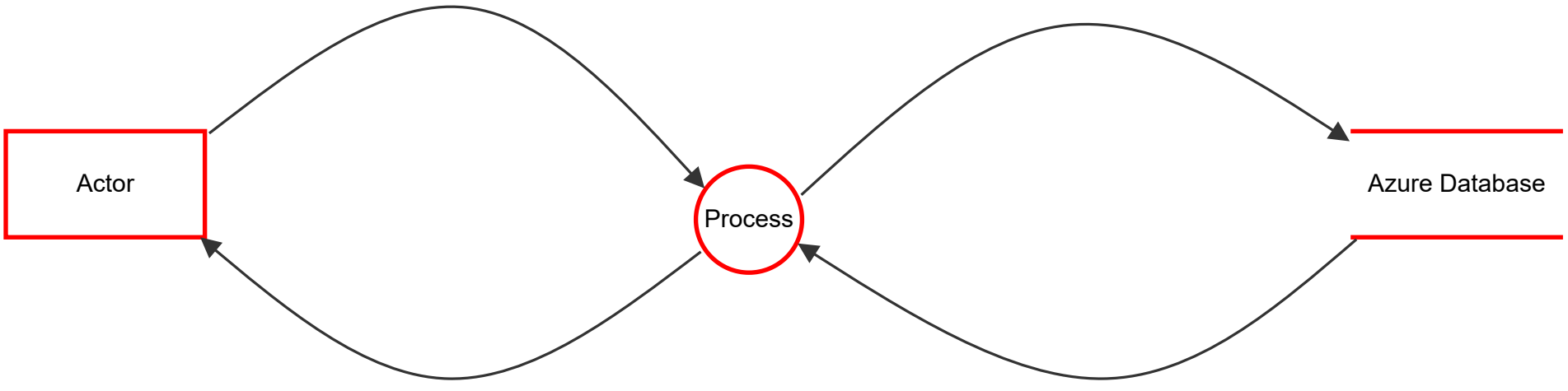
High level system description

Sign Language Detection App

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	0
Open / Medium Priority	10
Open / Low Priority	0
Open / Unknown Priority	0

Sign Language Detection App



Sign Language Detection App

Process (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Improper Validation Logic	Elevation of privilege	Medium	Open		Adversary may bypass critical steps or perform actions on behalf of other users due to improper validation logic	Lock down administrative interfaces. Enforce sequential step order in business logic. Implement proper authorization and least privilege principle. Don't base logic on request parameters. Content and resources shouldn't be enumerable.
8	Weak Encryption or Hashing	Information disclosure	Medium	Open		Adversary can reverse weakly encrypted or hashed content	Don't expose security details in error messages. Implement default error handling. Set deployment method to Retail in IIS. Link removed Use approved encryption algorithms and key lengths. Use approved random number generators. Verify X.509 certificates.
9	Information Disclosure through Robots	Information disclosure	Medium	Open		Adversary can gain access to certain pages	Lock down administrative interfaces.
10	Sniffing Traffic	Spoofing	Medium	Open		Adversary can gain access to sensitive information through error messages	Don't expose security details in error messages. Link Implement default error handling. Link Set deployment method to Retail in IIS. Link Exceptions should fail safely. Link Disable tracing and debugging before deployment. Link Implement controls to prevent username enumeration. Link

Actor (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Cross-Site Scripting (XSS) Vulnerability	Spoofing	Medium	Open		Adversary can perform actions on behalf of other users due to lack of controls against cross-domain requests	Ensure UI Redressing or clickjacking defenses for authenticated ASP.NET pages. Restrict origins if CORS is enabled. Mitigate CSRF attacks.
5	Improper Validation Logic	Spoofing	Medium	Open		Elevation of Privilege	Provide remediation for this threat or a reason if status is N/A
6	Sensitive Data in Browser Cache	Repudiation	Medium	Open		Adversary may gain access to sensitive data from uncleared browser cache	Ensure that sensitive content is not cached on the browser.

Azure Database (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Sensitive Data in Log Files	Information disclosure	Medium	Open		Adversary may gain access to sensitive data from log files	Don't log sensitive user data. Restrict access to audit and log files.
2	Unmasked Sensitive Data	Information disclosure	Medium	Open		Adversary may gain access to unmasked sensitive data	Mask sensitive data displayed on user screens.
3	Repudiation	Repudiation	Medium	Open		Attacker can deny the malicious act and remove the attack footprints leading to repudiation issues	Ensure that auditing and logging are enforced on the application. Ensure that log rotation and separation are in place. Restrict access to audit and log files. Ensure that User Management Events are Logged.

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