Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Wed Nov 20 2024

Executive Summary

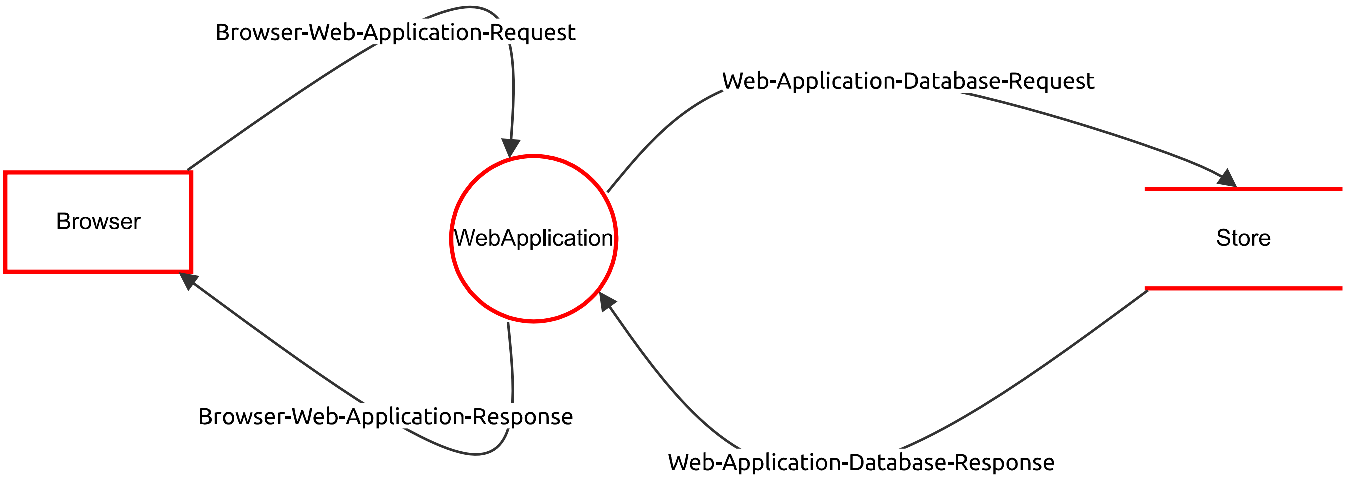
High level system description

Not provided

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

SportNewsWebResource


Browser-Web-Application-Request
Web-Application-Database-Request
Browser
WebApplication
Store
Browser-Web-Application-Response
Web-Application-Database-Response

SportNewsWebResource

Browser (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can spoof user identity in the browser	Spoofing	Medium	Open		An adversary can spoof the user's identity in the browser by manipulating authentication cookies or headers, impersonating the user and gaining unauthorized access to sensitive data or functionality.	Provide remediation for this threat or a reason if status is N/A

WebApplication (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	An adversary can inject malicious content into the web application's response	Tampering	Medium	Open		An adversary can inject malicious scripts or code into the web application's response to the browser, enabling the execution of cross-site scripting (XSS) attacks or redirecting users to phishing sites.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can intercept and modify responses from the web application to the browser	Tampering	Medium	Open		An adversary can modify the response data sent from the web application to the browser, altering content such as error messages, session data, or application logic, potentially confusing users or impacting functionality.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can compromise user session data during the response from the web application	Information disclosure	Medium	Open		An adversary could steal session cookies or tokens during the response from the web application, leading to session hijacking and unauthorized access to the user's account.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can exploit vulnerable input validation in requests sent from the browser	Tampering	Medium	Open		An adversary can exploit weak input validation in the web application by injecting malicious payloads in requests from the browser, leading to SQL injection, code execution, or other types of exploits.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can compromise user session data during the response from the web application	Information disclosure	Medium	Open		An adversary could steal session cookies or tokens during the response from the web application, leading to session hijacking and unauthorized access to the user's account.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can alter database queries initiated by the web application	Tampering	Medium	Open		An adversary with access to the web application can modify database queries, potentially causing unauthorized data changes, data leaks, or performance issues within the database.es.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can initiate a DoS attack on the database through malicious requests	Denial of service	Medium	Open		An adversary can send malicious or malformed requests from the web application to the database, causing it to overload and become unavailable, resulting in denial of service to legitimate users.	Provide remediation for this threat or a reason if status is N/A

Store (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	An adversary can intercept database responses containing sensitive data	Information disclosure	Medium	Open		An adversary can intercept and view unencrypted responses from the database, exposing sensitive data such as passwords, personal information, or confidential records.	Provide remediation for this threat or a reason if status is N/A
2	An adversary can manipulate database responses to the web application	Tampering	Medium	Open		An adversary can tamper with the responses from the database to the web application, potentially altering query results or injecting false data into the application, leading to incorrect application behavior or logic errors.	Provide remediation for this threat or a reason if status is N/A

Browser-Web-Application-Request (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web-Application-Database-Response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Browser-Web-Application-Response (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web-Application-Database-Request (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations