Dragon_DFD

Owner: Nikitin
Reviewer: N
Contributors:
Date Generated: Fri Oct 18 2024

Executive Summary

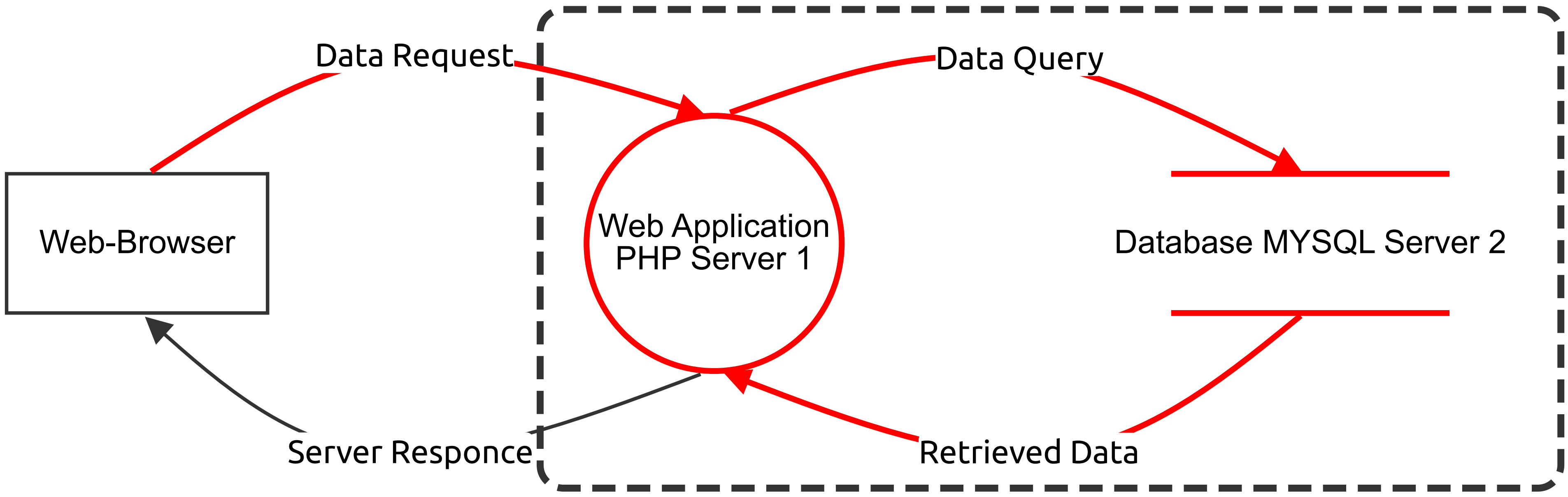
High level system description

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

Dragon_DFD_Stride



Dragon_DFD_Stride

Web Application

PHP Server 1 (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can get access to a user's session due to improper logout and timeout	Spoofing	Medium	Open		The session cookies is the identifier by which the server knows the identity of current user for each incoming request. If the attacker is able to steal the user token he would be able to access all user data and perform all actions on behalf of user.	Provide remediation for this threat or a reason if status is N/A
1	An adversary can get access to a user's session due to insecure coding practices	Spoofing	Medium	Open		The session cookies is the identifier by which the server knows the identity of current user for each incoming request. If the attacker is able to steal the user token he would be able to access all user data and perform all actions on behalf of user.	Provide remediation for this threat or a reason if status is N/A
1	Attacker can deny the malicious act and remove the attack foot prints leading to repudiation issues	Repudiation	Medium	Open		Proper logging of all security events and user actions builds traceability in a system and denies any possible repudiation issues. In the absence of proper auditing and logging controls, it would become impossible to implement any accountability in a system	Provide remediation for this threat or a reason if status is N/A
1	An adversary can create a fake website and launch phishing attacks	Spoofing	Medium	Open		An adversary can create a fake website and launch phishing attacks	Provide remediation for this threat or a reason if status is N/A

Web-Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Database MYSQL Server 2 (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can deny actions performed on Database MYSQL Server 2 due to a lack of auditing.	Repudiation	Medium	Open		An adversary can deny actions performed on Database MYSQL Server 2 due to a lack of auditing.	Provide remediation for this threat or a reason if status is N/A

Server Responce (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Query (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can read confidential data due to weak connection string configuration.	Information disclosure	Medium	Open		An adversary can read confidential data due to weak connection string configuration.	Provide remediation for this threat or a reason if status is N/A

Data Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can deface the target web application by injecting malicious code or uploading dangerous files	Tampering	Medium	Open		Website defacement is an attack on a website where the attacker changes the visual appearance of the site or a webpage.	Provide remediation for this threat or a reason if status is N/A
1	An adversary can gain access to sensitive data stored in Web App's config files	Tampering	Medium	Open		An adversary can gain access to the config files. and if sensitive data is stored in it, it would be compromised.	Provide remediation for this threat or a reason if status is N/A

Retrieved Data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	An adversary can gain access to sensitive data by performing SQL injection through Web App	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. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.	Provide remediation for this threat or a reason if status is N/A
1	An adversary can reverse weakly encrypted or hashed content	Information disclosure	Medium	Open		An adversary can reverse weakly encrypted or hashed content	Provide remediation for this threat or a reason if status is N/A