BammyCyberTech Web App

Owner: Bamidele Olaleke
Reviewer: Prof Ali Sanusi
Contributors:
Date Generated: Fri Nov 21 2025

Executive Summary

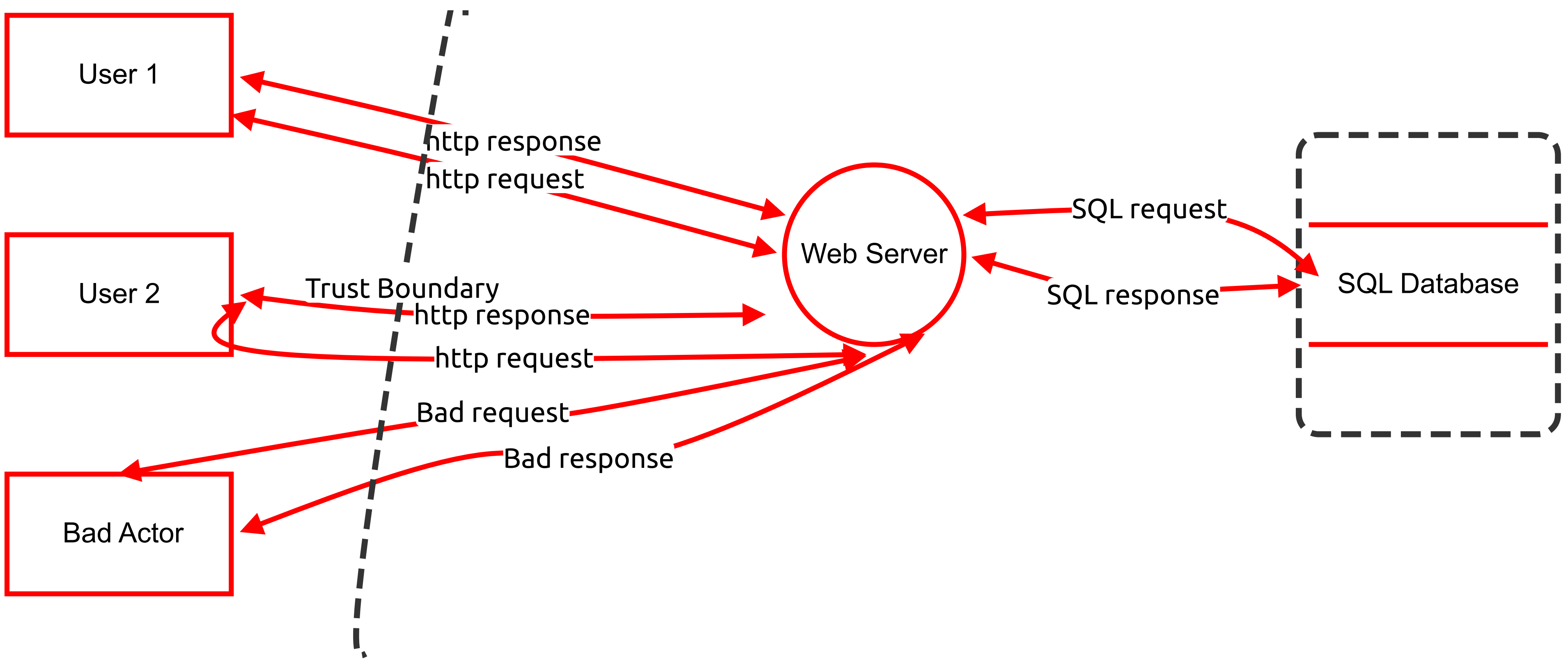
High level system description

Not provided

Summary

Total Threats	38
Total Mitigated	0
Total Open	38
Open / Critical Severity	0
Open / High Severity	0
Open / Medium Severity	0
Open / Low Severity	0
Open / TBD Severity	38

DFD for Bammy CyberTech Web App



DFD for Bammy CyberTech Web App

Web Server (Process)

Description: Web host server

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Web Server	Spoofing	TBD	Open		Impersonating another user or system to gain unauthorized access.	Strong authentication (MFA, biometrics, tokens) Secure password policies Use certificates and mutual authentication Validate all identities before granting access
6	Web Server	Tampering	TBD	Open		Unauthorized modification of data or systems	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
7	Web Server	Repudiation	TBD	Open		Performing actions without accountability or the ability to deny actions due to lack of logs.	Detailed auditing and logging Secure log storage Non-repudiation techniques (digital signatures, timestamps) Monitoring and SIEM tools
8	Web server	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services
9	Web server	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting
10	Web Server	Elevation of privilege	TBD	Open		Gaining higher-level access than permitted, often leading to full system compromise	Enforce least privilege Role-Based Access Control (RBAC) Privileged Access Management (PAM) Patch OS and applications Secure coding practices

User 1 (Actor)

Description: authenticated/unauthenticated user

Number	Title	Type	Severity	Status	Score	Description	Mitigations
11	User 1	Spoofing	TBD	Open		Impersonating another user or system to gain unauthorized access.	Strong authentication (MFA, biometrics, tokens) Secure password policies Use certificates and mutual authentication Validate all identities before granting access
12	User 1	Repudiation	TBD	Open		Performing actions without accountability or the ability to deny actions due to lack of logs.	Detailed auditing and logging Secure log storage Non-repudiation techniques (digital signatures, timestamps) Monitoring and SIEM tools

User 2 (Actor)

Description: Authenticated/Unauthenticated user

Number	Title	Type	Severity	Status	Score	Description	Mitigations
13	New STRIDE threat	Spoofing	TBD	Open		Impersonating another user or system to gain unauthorized access	Strong authentication (MFA, biometrics, tokens) Secure password policies Use certificates and mutual authentication Validate all identities before granting access
14	New STRIDE threat	Repudiation	TBD	Open		Performing actions without accountability or the ability to deny actions due to lack of logs.	Detailed auditing and logging Secure log storage Non-repudiation techniques (digital signatures, timestamps)

Bad Actor (Actor)

Description: Authenticated/authenticated user

Number	Title	Type	Severity	Status	Score	Description	Mitigations
15	New STRIDE threat	Spoofing	TBD	Open		Impersonating another user or system to gain unauthorized access	Strong authentication (MFA, biometrics, tokens) Secure password policies Use certificates and mutual authentication
16	Bad User	Repudiation	TBD	Open		Performing actions without accountability or the ability to deny actions due to lack of logs.	Detailed auditing and logging Secure log storage Non-repudiation techniques (digital signatures, timestamps) Monitoring and SIEM tools

http request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
17	http	Tampering	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS)
18	http	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services
19	New STRIDE threat	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services

http response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
20	http response	Tampering	TBD	Open		Unauthorized modification of data or systems	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
21	New STRIDE threat	Information disclosure	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF
22	http response	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting

http response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
35	New STRIDE threat	Tampering	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures
36	New STRIDE threat	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services

Number	Title	Type	Severity	Status	Score	Description	Mitigations
37	New STRIDE threat	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting

http request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
38	user 2	Tampering	TBD	Open		Unauthorized modification of data or systems.	Access controls and file permissions Input validation

Bad request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
32	bad request	Tampering	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
33	Bad request	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs
34	Bad request	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting

Bad response (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
29	Bad response	Tampering	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
30	New STRIDE threat	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control

Number	Title	Type	Severity	Status	Score	Description	Mitigations
31	Bad actor	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services

SQL response (Data Flow)

Description: Storage

Number	Title	Type	Severity	Status	Score	Description	Mitigations
23	SQL response	Tampering	TBD	Open		Unauthorized modification of data or systems.	Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
24	New STRIDE threat	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services
25	SQL R	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting

SQL request (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
26	New STRIDE threat	Tampering	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
27	New STRIDE threat	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services
28	SQL	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	DDoS protection services Resource monitoring and alerting

SQL Database (Store)

Description: store everything

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	SQL Database	Tampering	TBD	Open		Impersonating another user or system to gain unauthorized access	Strong authentication (MFA, biometrics, tokens) Secure password policies Use certificates and mutual authentication Validate all identities before granting access
2	SQL Database	Repudiation	TBD	Open		Unauthorized modification of data or systems.	Use hashing and integrity checks (e.g., SHA-256) Digital signatures Secure protocols (TLS/HTTPS) Access controls and file permissions Input validation
3	SQL database	Information disclosure	TBD	Open		Exposing sensitive or confidential data to unauthorized parties.	Encryption at rest and in transit Data classification and access control Secure APIs Tokenization and masking Patch vulnerable services
4	SQL database	Denial of service	TBD	Open		Disrupting system availability, making services unavailable to legitimate users.	Rate limiting and throttling Firewalls and WAF Load balancing and redundancy DDoS protection services Resource monitoring and alerting