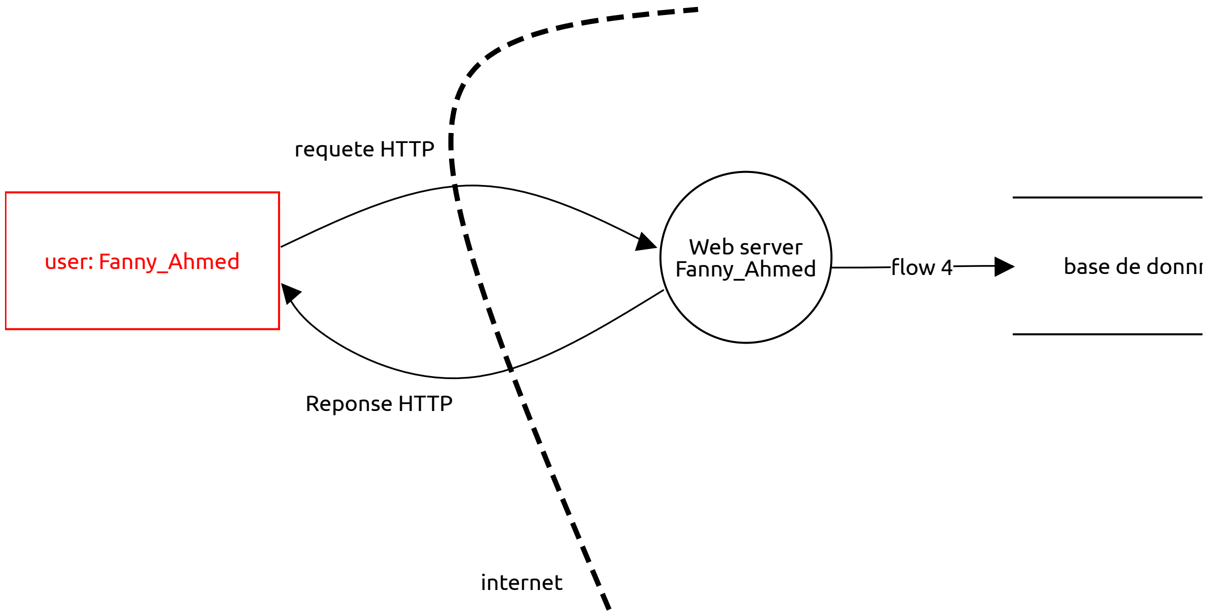
Threat model report for Demo Threat Model

Owner:
Mike Goodwin
Reviewer:
Jane Smith
Contributors:
Tom Brown; Albert Moneypenny

High level system description

A sample model of a web application, with a queue-decoupled background process.

Web app fanny_ahmed



Web server Fanny_Ahmed (Process)

Description:

No threats listed.

user: Fanny_Ahmed (External Actor)

Description:

Denial of service

Denial of service, Open, Medium Priority

Description:
An attacker can intentionally overload the application or service by sending a high volume of requests or exploiting resource-intensive operations, causing degradation or complete unavailability of the system for legitimate users.
This can lead to loss of availability, reputation damage, and service-level agreement (SLA) violations.

Mitigation:
Implement rate limiting and throttling to restrict excessive requests from the same source.
Use Web Application Firewalls (WAF) to detect and block suspicious traffic patterns.
Monitor system performance and set alerts for unusual spikes in usage.
Employ caching and load balancing to reduce server load.
Consider CAPTCHAs or challenge-response mechanisms to prevent automated abuse.

requete HTTP (Data Flow)

Description:

No threats listed.

Reponse HTTP (Data Flow)

Description:

No threats listed.

base de donnnée (Data Store)

Description:

No threats listed.

flow 4 (Data Flow)

Description:

No threats listed.