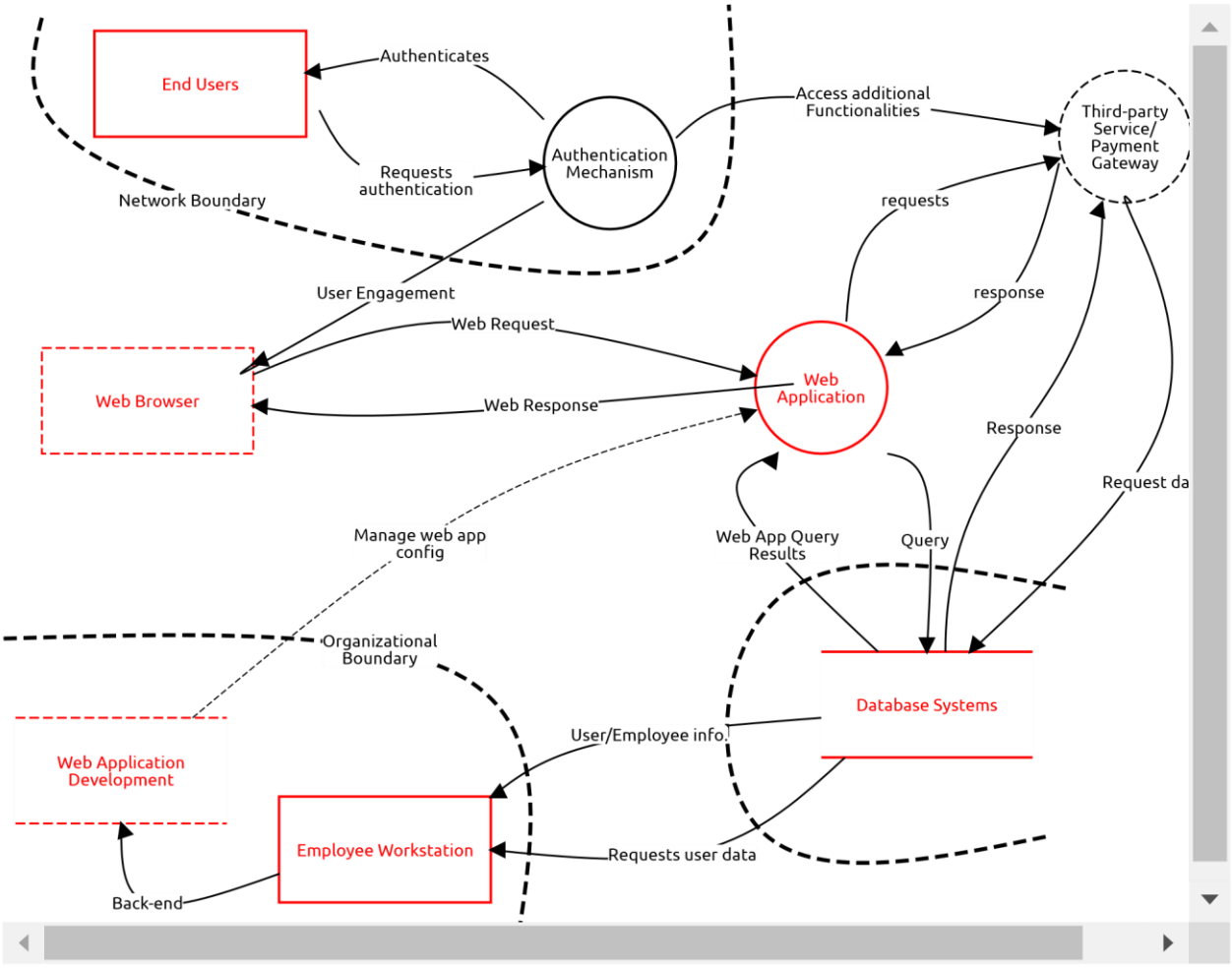
Threat model report for Demo Threat Model

Owner:
Arpit Sharma
Reviewer:
SWAT Alliance
Contributors:
Tom Brown; Albert Moneypenny

High level system description

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

Main Request Data Flow



Database Systems (Data Store)

Description:

Unauthorised access

Information disclosure, Mitigated, High Priority

Description:
An attacker could make an query call on the DB,

Mitigation:
Require all queries to be authenticated.

Credential theft

Information disclosure, Open, Medium Priority

Description:
An attacker could obtain the DB credentials ans use them to make unauthorised queries.

Mitigation:
Use a rewall to restrict access to the DB to only the Background Worker IP address.

Hardware Failure

Tampering, Open, High Priority

Description:
Natural disaster, Human Error

Mitigation:
Several location, Backup

Web Application (Process)

Description:

DoS

Denial of service, Open, Medium Priority

Description:

Mitigation:
IDS, IPS

XSS

Information disclosure, Open, Medium Priority

Description:

Mitigation:
Input Validation

SQL Injection

Spoofing, Open, Medium Priority

Description:

Mitigation:
Parametrized Query, Input Validation

Web Request (Data Flow)

Description:

Data ow should use HTTP/S

Information disclosure, Mitigated, High Priority

Description:
These requests are made over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide con dentiality and integrity. HTTP should not be supported.

Web Response (Data Flow)

Description:

Data ow should use HTTP/S

Information disclosure, Mitigated, High Priority

Description:
These responses are over the public internet and could be intercepted by an attacker.

Mitigation:
The requests should require HTTP/S. This will provide con dentiality and integrity. HTTP should not be supported.

Web App Query Results (Data Flow)

Description:

No threats listed.

End Users (External Actor)

Description:

Social Engineering

Spoofing, Mitigated, Low Priority

Description:

Mitigation:
Awareness and Training

Malware Attacks

Information disclosure, Mitigated, Medium Priority

Description:

Mitigation:
Encryption, MFA

Data Theft

Confidentiality, Open, Medium Priority

Description:

Mitigation:

Employee Workstation (External Actor)

Description:

Insider Threat

Tampering, Open, High Priority

Description:
Employees who have access to the online banking platform can intentionally or unintentionally leak sensitive information, perform unauthorized transactions or manipulate data.

Mitigation:
Access Control

Query (Data Flow)

Description:

No threats listed.

Authentication Mechanism (Process)

Description:

No threats listed.

Authenticates (Data Flow)

Description:

No threats listed.

Requests authentication (Data Flow)

Description:

No threats listed.

User Engagement (Data Flow)

Description:

No threats listed.

Back-end (Data Flow)

Description:

No threats listed.

Access additional Functionalities(Data Flow)

Description:

No threats listed.

Request data (Data Flow)

Description:

No threats listed.

User/Employee info. (Data Flow)

Description:

No threats listed.

Requests user data(Data Flow)

Description:

No threats listed.

Response (Data Flow)

Description:

No threats listed.

response (Data Flow)

Description:
Provides interface to engage with the user and displays user data over the web app

No threats listed.

requests (Data Flow)

Description:

No threats listed.

Web Application Development (out of scopeData Store)

Description:

Out of scope reason:

Web Browser (out of scope External Actor)

Description:

Out of scope reason:

Manage web app con g (out of scopeData Flow)

Description:

Out of scope reason:
This data ow represents a read from the le system

Third-party Service/ Payment Gateway (out of scopeProcess)

Description:
External service providers, such as payment gateways or cloud storage providers, that interact with the online banking platform to provide additional functionality.

Out of scope reason: