Secure Programming

Lab1

Threat Modelling

Steps

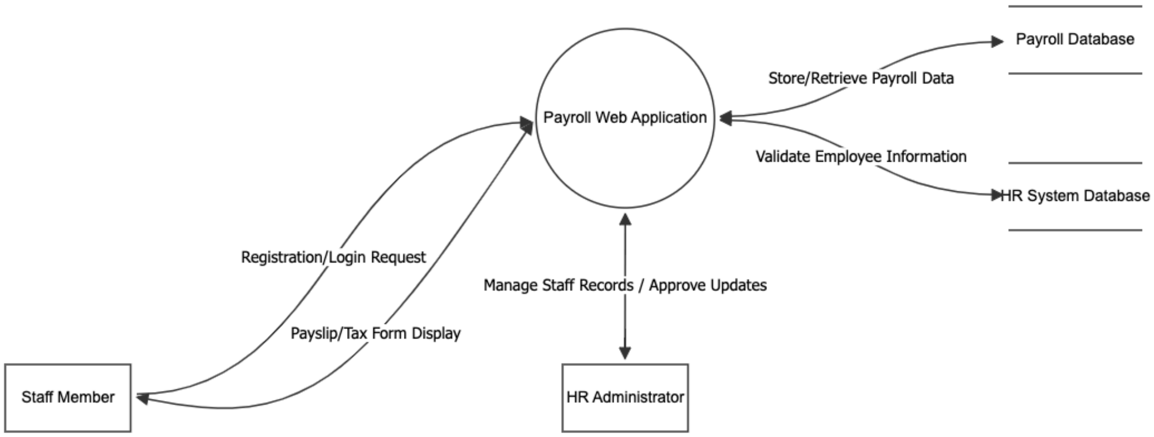
Step 1: Identify security objectives:

- What type of data will be published/ held?
  - **Personal data:** Name, email, staff ID, address.
  - **Sensitive data:** Bank account details, tax number, payslips, tax forms.
  - **Authentication data:** Username/password (credentials).
- Are there any data regulations? e.g. medical/legal/ financial/ privacy?
  - **GDPR** (personal & financial info).
  - **Financial data handling regulations** (bank details, tax records).
- Will the site hold private/ sensitive data?
  - **Confidentiality:** Prevent unauthorized access (staff data, payslips, tax forms).
  - **Integrity:** Ensure personal/bank/tax details aren’t tampered with.
  - **Availability:** Ensure staff can always access payslips/tax forms, especially during payroll deadlines.
- Will this generate a large revenue stream?
  - **Direct impact on employees’ finances** (payslips, tax).
  - **Reputational damage** if compromised.
  - **Regulatory fines** if mishandled.

  In other words, what are the issues around Confidentiality, Integrity and Availability?

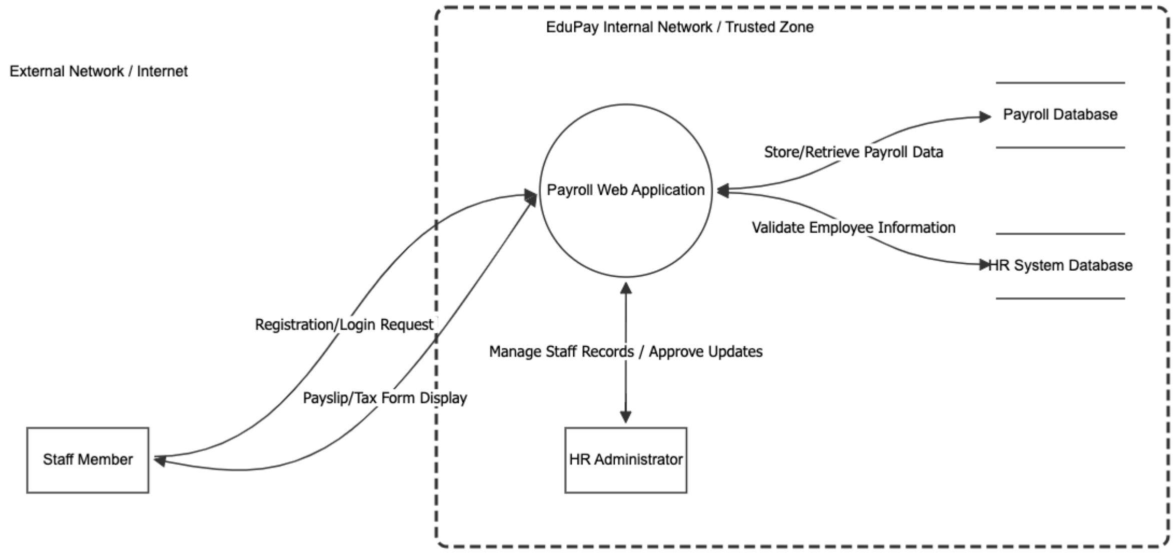
  → The EduPay payroll portal handles highly sensitive personal and financial data, so confidentiality is critical to prevent unauthorized access to staff information like bank details or tax records. Integrity must be maintained to ensure that payslips, personal information, and financial data are accurate and cannot be tampered with. Availability is essential so employees can reliably access their payroll information and tax forms without downtime, especially during pay periods.

Step 2: Create an application overview


Payroll Database
Store/Retrieve Payroll Data
Payroll Web Application
Validate Employee Information
HR System Database
Registration/Login Request
Manage Staff Records / Approve Updates
Payslip/Tax Form Display
Staff Member
HR Administrator

- Draw out a rough sketch of the new subsystem
    - The system includes a web application that communicates with two internal databases – the Payroll Database and the HR System Database – separated from the public Internet by a trust boundary. Staff members access the portal via their web browsers, while HR administrators and system components operate within the secure internal network.
- Outline the users in the system and their roles
    - **Staff Member:** Registers and logins in to view payslips, download tax forms, and update personal or banking details.
    - **HR Administrator:** Verifies employee information, manages payroll data, and approves updates submitted by staff.
- Identify the technologies (system components – servers, databases, etc.)
    - **Client Layer:** Web browser accessed by staff members over HTTPS.
    - **Application Layer:** Payroll Web Application running on a secure web server.
    - **Payroll Database:** Stores staff credentials, payslips, tax data, and personal information.
    - **HR System Database:** Validates employee records against existing HR data.
    - **Network Layer:** Protected internal EduPay network with firewalls and TLS-encrypted connections between components.
- Identify possible security mechanisms
    - **Authentication and Authorization:** Strong password policy, multi-factor authentication, and role-based access control.
    - **Encryption:** HTTPS/TLS for all external communications and encryption at rest for sensitive data in databases.
    - **Input Validation:** To prevent SQL injection, XSS, and data manipulation attacks.
    - **Access Control:** Principle of least privilege for users and services.
    - **Backup and Recovery:** Regular encrypted backups and redundancy to ensure system availability.

Step 3: Decompose your application


EduPay Internal Network / Trusted Zone
External Network / Internet
Payroll Database
Store/Retrieve Payroll Data
Payroll Web Application
Validate Employee Information
HR System Database
Registration/Login Request
Manage Staff Records / Approve Updates
Payslip/Tax Form Display
Staff Member
HR Administrator

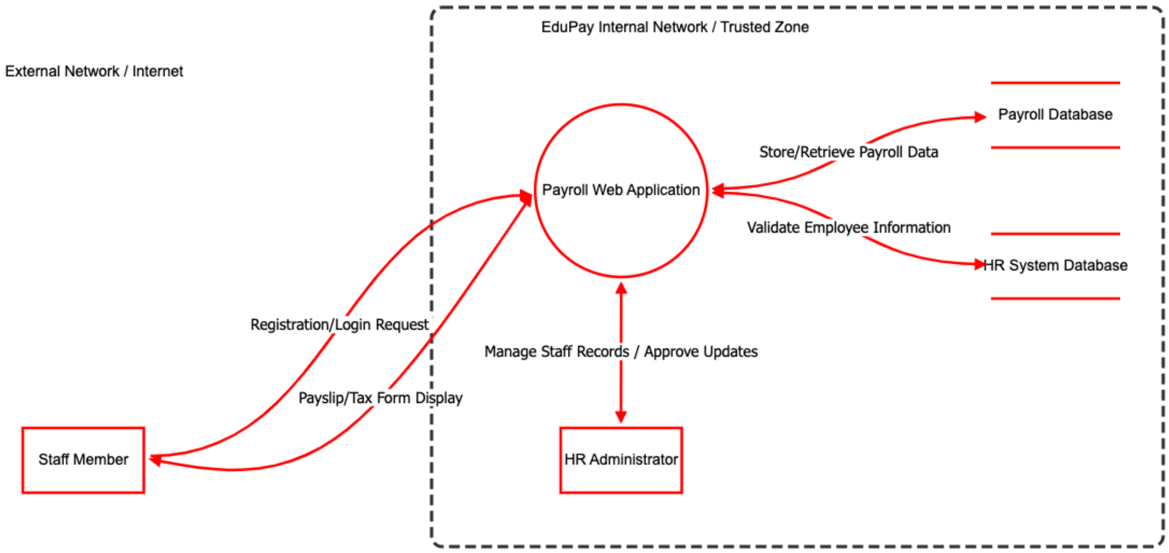
- Identify trust boundaries, entry/ exit points
  - **External Network / Internet:** Contains Staff Members who access the portal from personal or institutional devices (Communication with the EduPay system occurs over HTTPS).
  - **EduPay Internal Network / Trusted Zone:** Contains the Payroll Web Application, Payroll Database, HR System Database, and HR Administrator (This zone is protected by firewalls, internal access controls, and encryption mechanisms).
- Identify data flows and draw a data flow diagram (Use MS Threat Model Tool or OWASP Threat Dragon)
  - **diagram above** ↑

Step 4: Identify threats

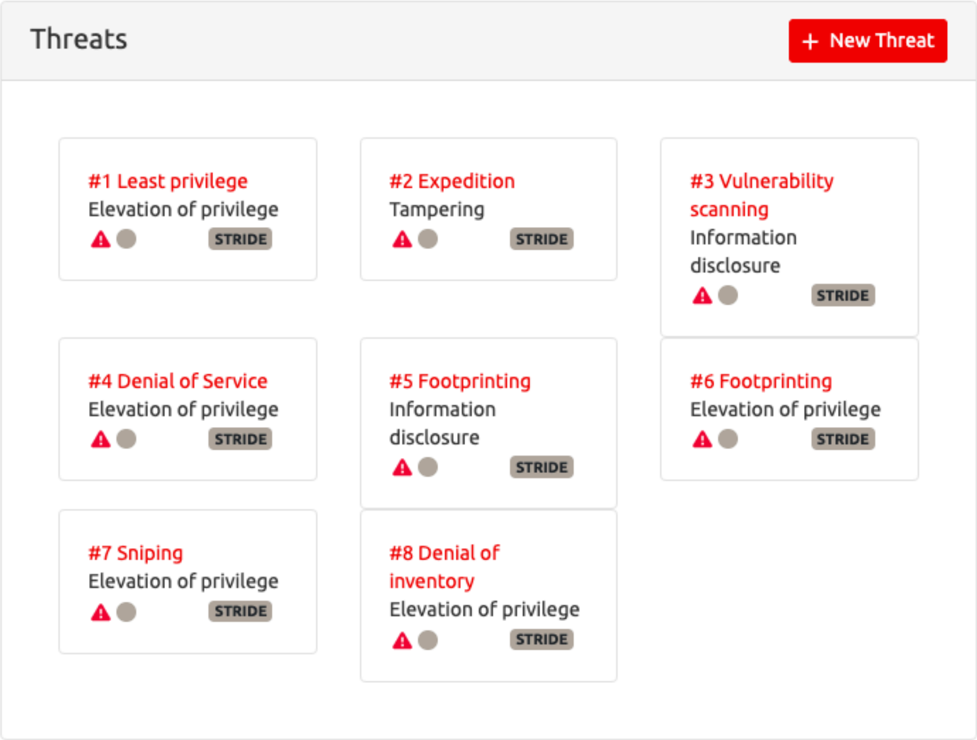
- Who might be interested in compromising the system? (organised criminals, hacktivists, competitors etc.)
  - **Organised cyber-criminals** — Steal bank and payroll data for financial gain (identity theft, fraud).
  - **Hacktivists** — Deface or leak data to protest education or payroll practices.
  - **Disgruntled employees / insiders** — Modify or delete payroll records, cause reputational or financial damage.
  - **Competitors** — Access internal processes or HR data to gain unfair advantage.
  - **Accidental threats** — User mistakes or misconfigurations that expose data unintentionally.

- What are the bad things that can happen? (e.g. stealing customer data)
    - Theft of staff **personal or financial data** (bank details, tax numbers).
    - **Credential compromise** leading to unauthorized account access.
    - **Tampering** with payslips, salary amounts, or tax information.
    - **Denial of Service** (DoS) preventing employees from accessing the portal.
    - **Data leakage** through insecure storage or weak encryption.
    - **Privilege escalation** by insiders or attackers.
    - **Reputational damage** and **GDPR non-compliance fines**.
- What impact would it have on the business?
    - **Loss of employee trust** and **reputation damage**.
    - **Financial loss** through fraud or ransomware.
    - **Legal penalties** for violating data-protection laws (e.g., GDPR).
    - **Operational disruption** if payroll services are offline.
- Try to decompose the subsystem into components and identify possible threats for each one
    - **Payroll Web Application (Process)**
        - SQL injection and command injection attacks.
        - Cross-site scripting (XSS) and unvalidated input.
        - Session hijacking and CSRF attacks.
        - Denial of service (DoS) through excessive requests.
        - Insufficient authentication or privilege escalation.
    - **Payroll Database (Data Store)**
        - Unauthorized access to payroll or banking data.
        - Tampering with payslips or salary records.
        - Data leakage or theft due to weak encryption.
        - Ransomware or deletion of records.
    - **HR System Database (Data Store)**
        - Exposure of employee data via insecure APIs.
        - Data corruption or modification during synchronization.
        - Lack of access controls for HR data queries.
    - **HR Administrator (Actor)**
        - Misuse of administrative privileges.
        - Insider data theft or accidental exposure.
        - Weak authentication for admin access.
    - **Staff Member (Actor)**
        - Credential theft through phishing or fake login pages.
        - Session hijacking using stolen cookies or tokens.
    - **Data Flows (Network Connections)**
        - Man-in-the-middle (MITM) interception across the Internet.
        - Unencrypted data transmission inside the internal network.
        - Packet sniffing or replay attacks.

Step 5: Identify vulnerabilities


EduPay Internal Network / Trusted Zone
External Network / Internet
Payroll Database
Store/Retrieve Payroll Data
Payroll Web Application
Validate Employee Information
HR System Database
Registration/Login Request
Manage Staff Records / Approve Updates
Payslip/Tax Form Display
Staff Member
HR Administrator

- Look at the system design to identify possible vulnerabilities
    - **Payroll Web Application (Process)**



Threats

#1 Least privilege
Elevation of privilege
⚠ ● STRIDE

#2 Expedition
Tampering
⚠ ● STRIDE

#3 Vulnerability scanning
Information disclosure
⚠ ● STRIDE

#4 Denial of Service
Elevation of privilege
⚠ ● STRIDE

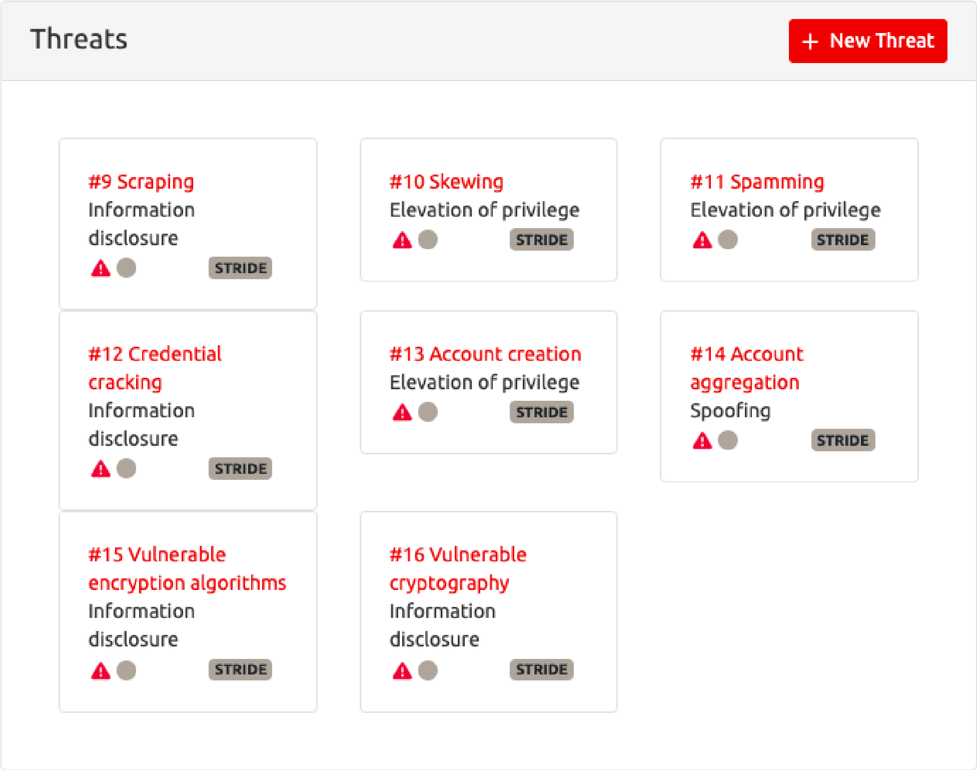
#5 Footprinting
Information disclosure
⚠ ● STRIDE

#6 Footprinting
Elevation of privilege
⚠ ● STRIDE

#7 Sniping
Elevation of privilege
⚠ ● STRIDE

#8 Denial of inventory
Elevation of privilege
⚠ ● STRIDE

- ### Payroll Database (Data Store)



#9 Scraping
Information disclosure
⚠ ● STRIDE

#10 Skewing
Elevation of privilege
⚠ ● STRIDE

#11 Spamming
Elevation of privilege
⚠ ● STRIDE

#12 Credential cracking
Information disclosure
⚠ ● STRIDE

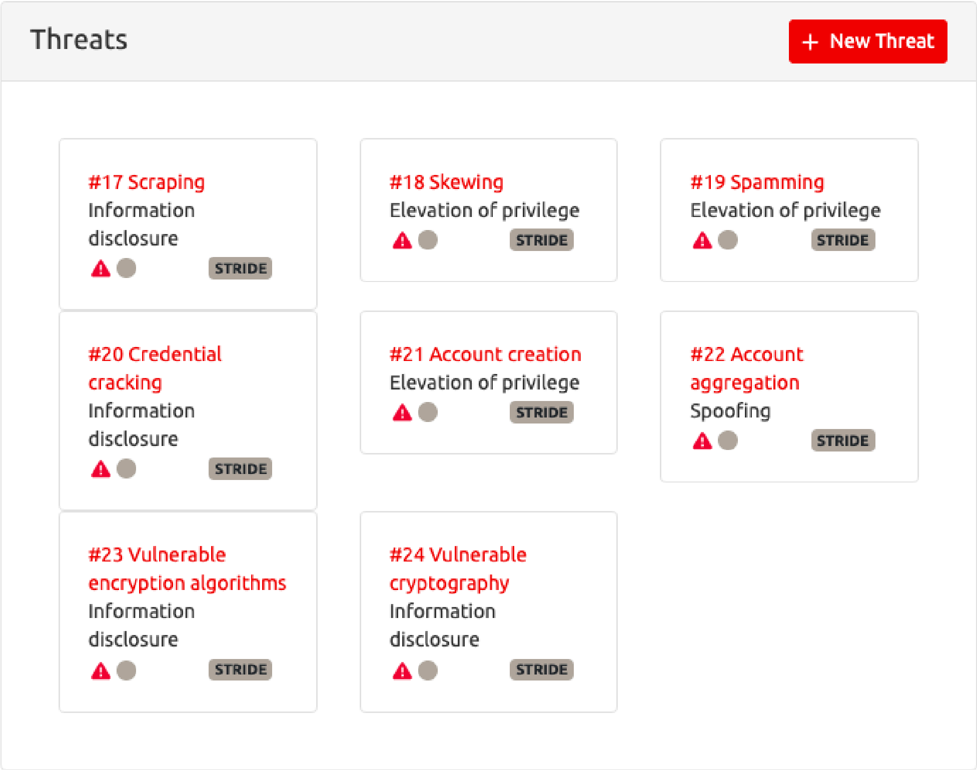
#13 Account creation
Elevation of privilege
⚠ ● STRIDE

#14 Account aggregation
Spoofing
⚠ ● STRIDE

#15 Vulnerable encryption algorithms
Information disclosure
⚠ ● STRIDE

#16 Vulnerable cryptography
Information disclosure
⚠ ● STRIDE

- ### HR System Database (Data Store)



#17 Scraping
Information disclosure
⚠ ● STRIDE

#18 Skewing
Elevation of privilege
⚠ ● STRIDE

#19 Spamming
Elevation of privilege
⚠ ● STRIDE

#20 Credential cracking
Information disclosure
⚠ ● STRIDE

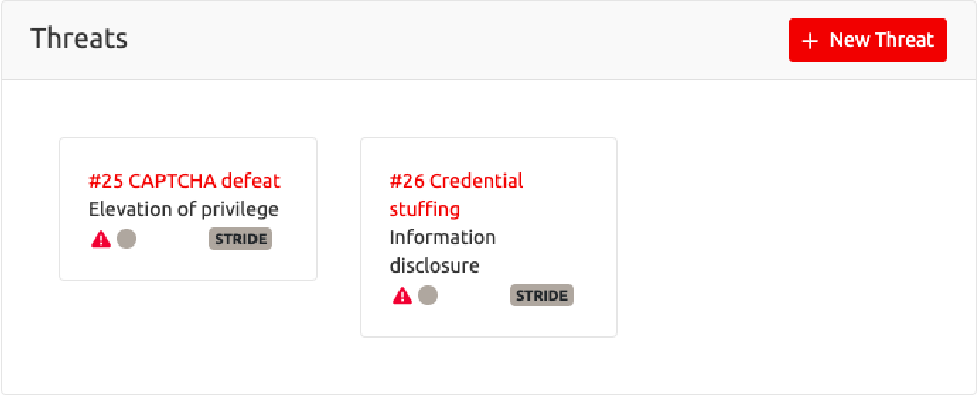
#21 Account creation
Elevation of privilege
⚠ ● STRIDE

#22 Account aggregation
Spoofing
⚠ ● STRIDE

#23 Vulnerable encryption algorithms
Information disclosure
⚠ ● STRIDE

#24 Vulnerable cryptography
Information disclosure
⚠ ● STRIDE

- ### HR Administrator (Actor)

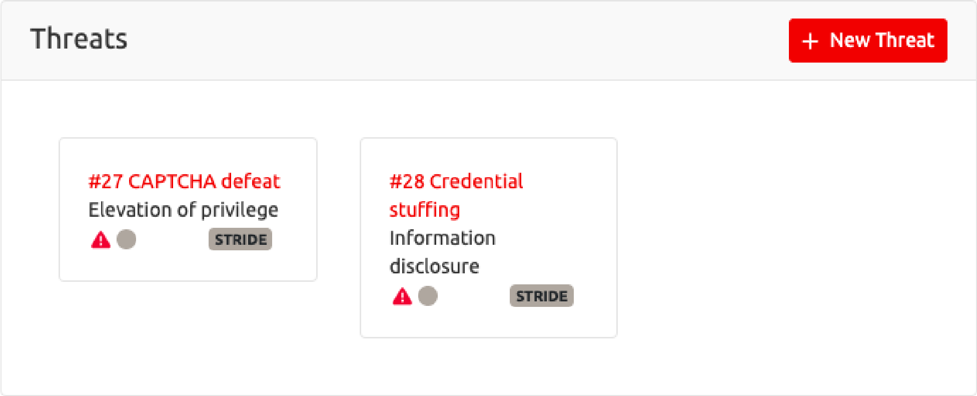


Threats

#25 CAPTCHA defeat
Elevation of privilege
STRIDE

#26 Credential stuffing
Information disclosure
STRIDE

- ### Staff Member (Actor)

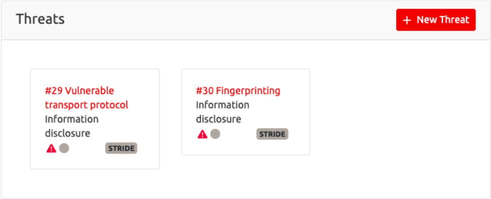


Threats

#27 CAPTCHA defeat
Elevation of privilege
STRIDE

#28 Credential stuffing
Information disclosure
STRIDE

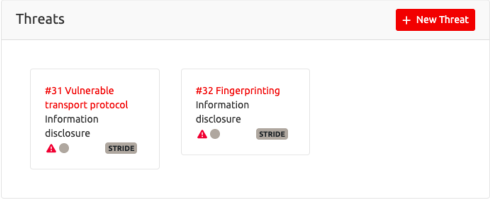
- ### Data Flows (Network Connections)



Threats

#29 Vulnerable transport protocol
Information disclosure
STRIDE

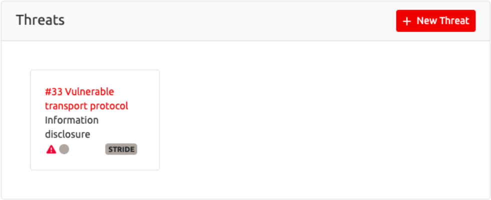
#30 Fingerprinting
Information disclosure
STRIDE



Threats

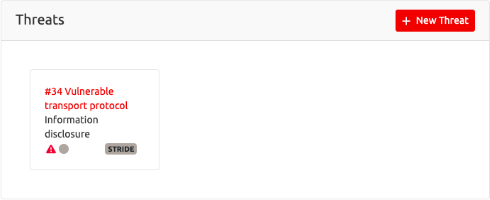
#31 Vulnerable transport protocol
Information disclosure
STRIDE

#32 Fingerprinting
Information disclosure
STRIDE



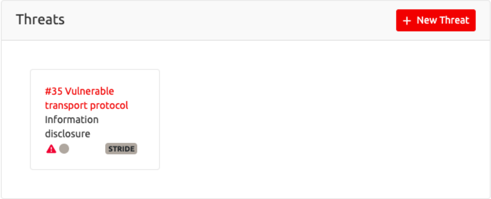
Threats

#33 Vulnerable transport protocol
Information disclosure
STRIDE



Threats

#34 Vulnerable transport protocol
Information disclosure
STRIDE



Threats

#35 Vulnerable transport protocol
Information disclosure
STRIDE