Enhance Your Security Posture with the Power of Threat Modelling

Danielle Dias
Senior Backend Engineer
at Flagstone

FLAGSTONE

FLAGSTONE

OWASP Bristol Chapter
November 2025

Security

Protection

Reputation

Enhance Your Security Posture

Threat Modelling: What and why?

How do you actually Threat Model?

Threat Modelling in Action

"If you fail to plan, you are planning to fail."

What are we building this sprint?

As a business customer,

I want to download a VAT receipt for my purchases,

So that I can claim back VAT and keep accurate financial records for accounting purposes.

Integrating Threat Modelling: Designing for Security

The Overlooked Aspect

Introducing Threat Modelling

"Threat modelling works to **identify**, **communicate**, and **understand threats and mitigations** within the context of **protecting** something of **value**."

The Open Worldwide Application Security Project (OWSAP) - Threat Modelling


Yahoo agrees to pay $50M in damages over biggest security breach in history
A NEW GOOGLE+ BLUNDER EXPOSED DATA FROM 52.5 MILLION USERS
Exactis said to have exposed 340 million records, more than Equifax breach
Facebook Breach Exposed Personal Data of Millions of Users
Hackers could find out your birthplace, religion, gender, and relationships. What you can do about it.
T-Mobile was hit by a data breach affecting around 2 million customers
Latest Facebook-related security breach finds millions of records exposed on Amazon servers
Hack of DNA Website Exposes Data From 92 Million Accounts
Quora says 100 million users hit by 'malicious' data breach

What’s at Stake?

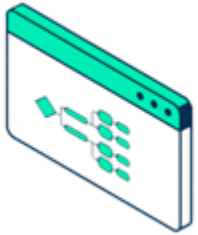
- **Financial Loss**
- **Infrastructure Costs**
- **Delays to Development**
- **Operational Strain**

Putting Threat Modelling into Action:

The Four-Question Framework

- Accessible & Effective
- Early Threat Identification
- Security by Design

The Four-Question Framework for Threat Modelling



1. What are we working on?

Building the diagram

2. What can go wrong?

Pinpoint the threats

3. What are we going to do about it?

Mitigating the threats

4. Did we do a good job?

Validating the design and reporting the process

iriusrisk: The Four-Question Framework for Threat Modelling

1 What are we working on?

- Whiteboarding
- Data Flow Diagrams
- Involves Multiple People

2 What can go wrong?

- Think Like an Attacker
- Collaborate
- Use Structured Approaches

3 What are we going to do about it?

- Evaluate and Prioritise Risks
- Track and Manage Risks
- Integrate Security into Development

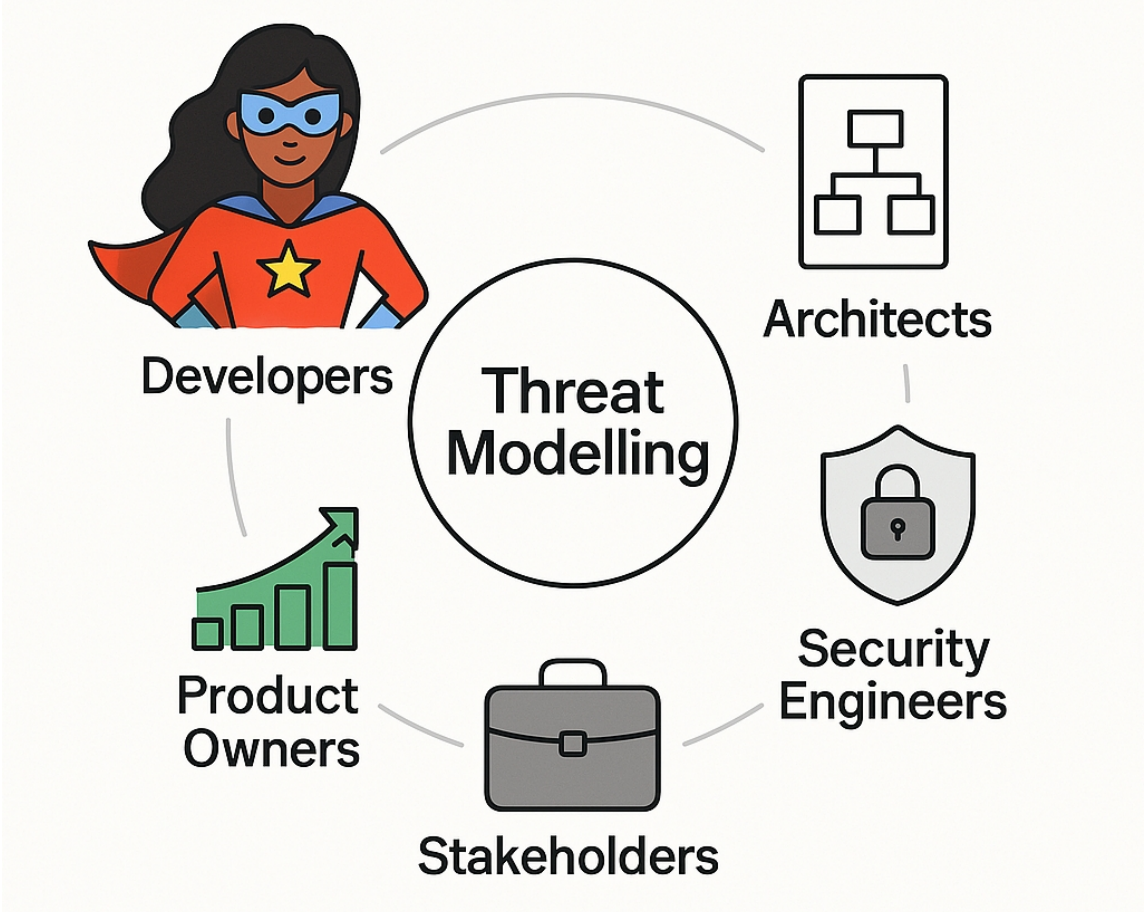
4 Did we do a good job?

- Evaluate the Security Approach
- Security checklist
- Continuous improvement

When to Carry Out Threat Modelling

- During Design
- Before Major Architecture Changes
- Security Reviews
- After Incidents

Who to Involve



Choosing the Right Approach

- **STRIDE**
  Categorise threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

- **PASTA**
  Risk-driven approach: Process for Attack Simulation and Threat Analysis

- **Attack Trees**
  Visualise attacker goals and paths

- **Security Checklists**
  Quick and repeatable prompts for identifying common security issues

Free and Open-Source Tools

- **OWASP Threat Dragon**

Open-source Threat Modelling platform with a user-friendly interface

- **IriusRisk Community Edition**

Comprehensive Threat Modelling tool with risk assessment capabilities

- **app.diagrams.net / draw.io**

Easy-to-use diagramming tool

What are we building this sprint?

As a business customer,

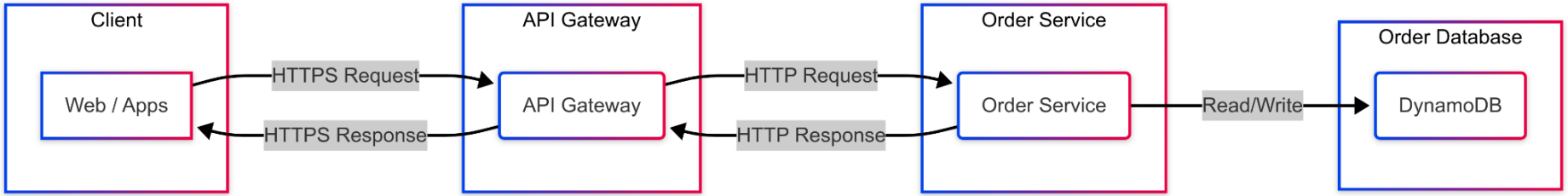
I want to download a VAT receipt for my purchases,

So that I can claim back VAT and keep accurate financial records for accounting purposes.

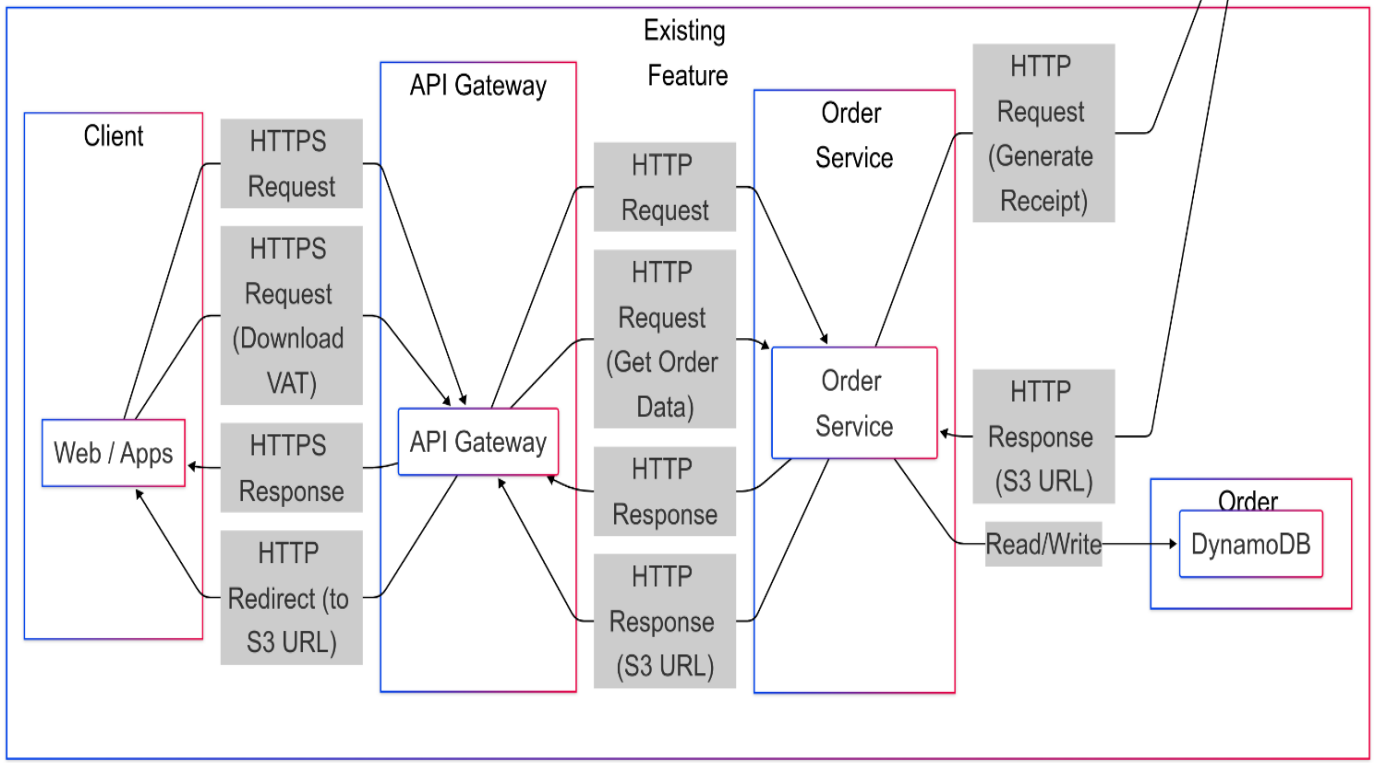
1 What are we working on?

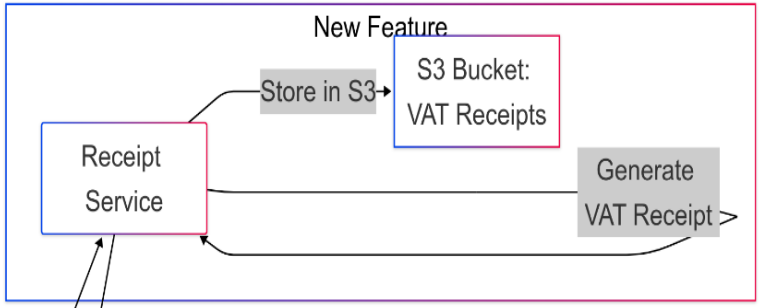
VAT Receipt Example

1 What are we working on?



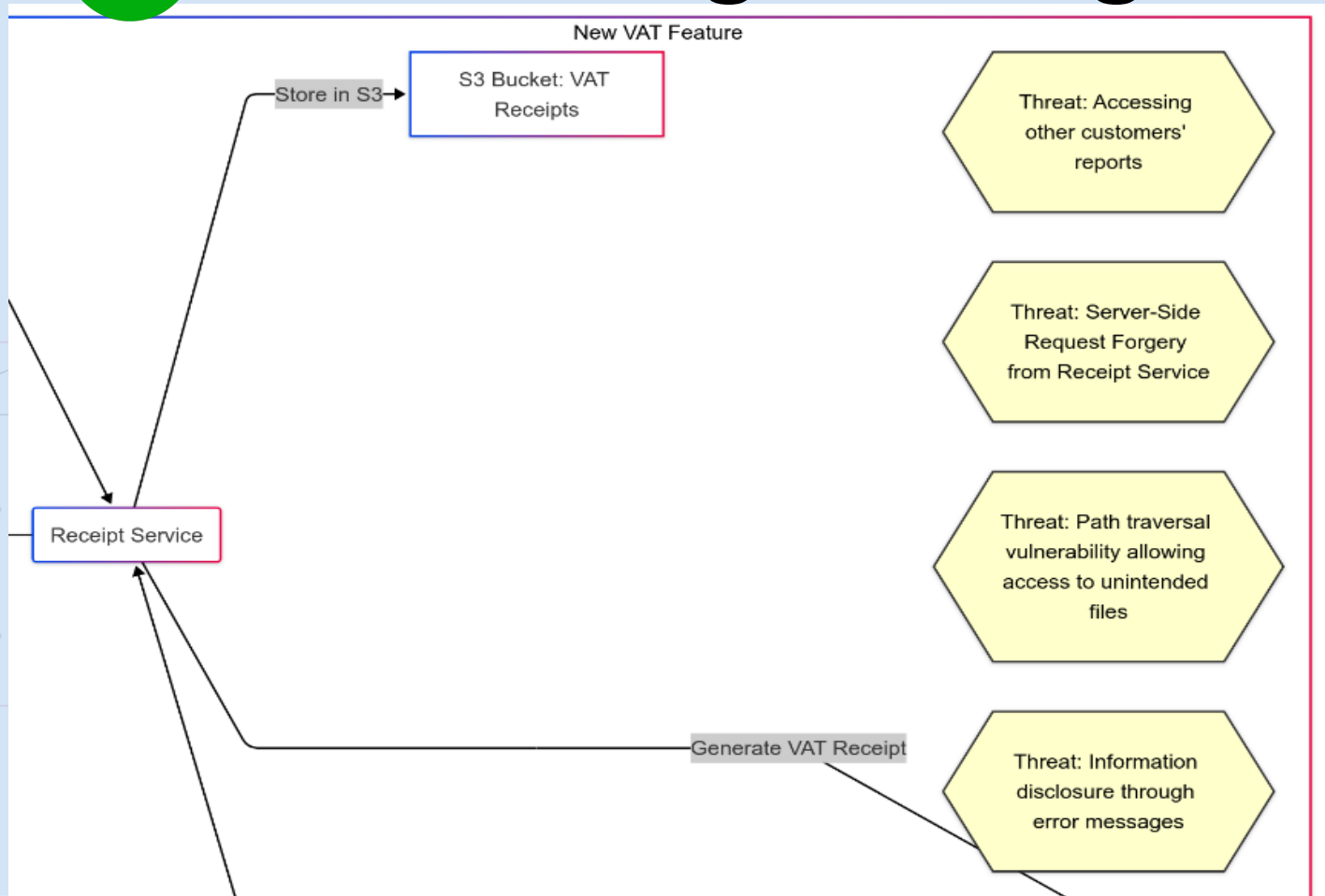
1 What are we working on?





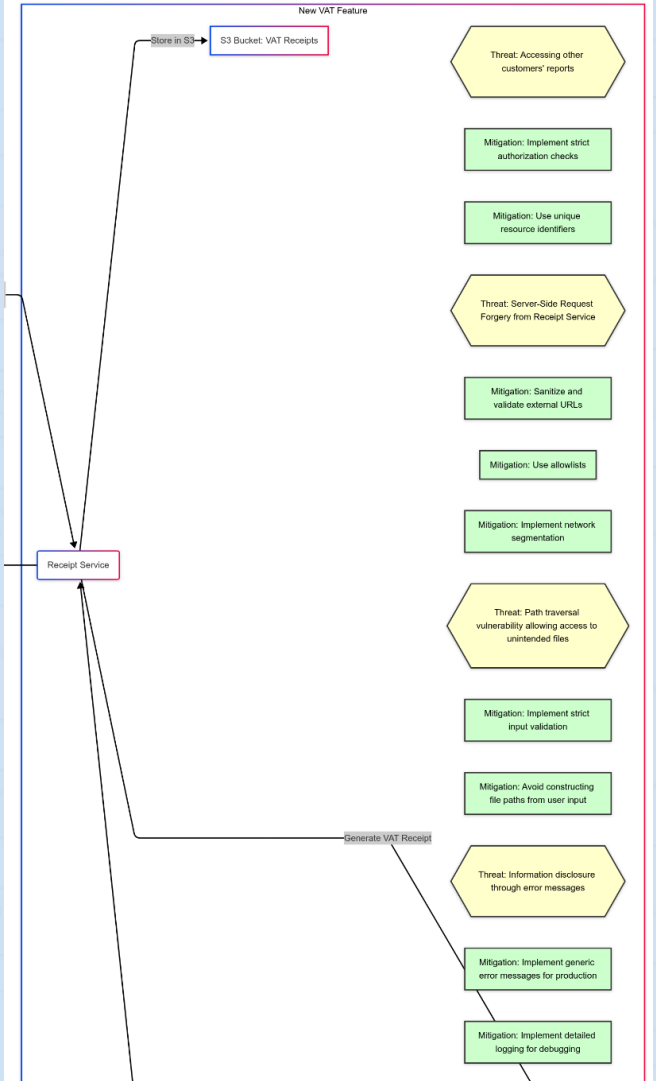
2 What can go wrong?

2 What can go wrong?



3 What are we going to do about it?

3 What are we going to do about it?



Threats, Mitigations, and Risk Levels

Threat ID	Threat	Mitigation	Risk Level
T1	DDoS on API Gateway	Implement rate limiting	High
T1	DDoS on API Gateway	Implement traffic shaping	High
T1	DDoS on API Gateway	Use a CDN	High
T2	Non-business user downloading report	Implement role-based access control	Medium
T2	Non-business user downloading report	Implement authentication	Medium
T3	Accessing other customers' reports	Implement strict authorization checks	Critical
T3	Accessing other customers' reports	Use unique resource identifiers	Critical

A Small Time Investment for Big Returns

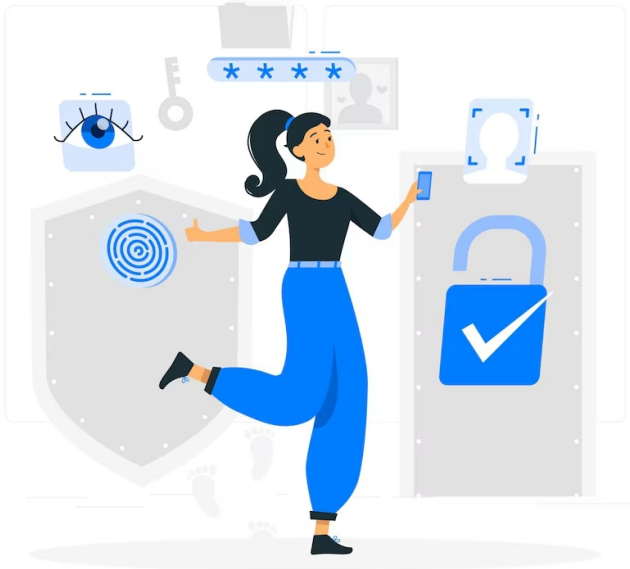
- Define Security Requirements
- Enhanced Understanding
- Cost Savings
- Spot Hidden Flaw
- Consider New Attack Vectors
- Better Quality and Design


BURN
BOOK
THREAT MODELLING IS JUST
WRITING ALL THE TERRIBLE THINGS
ATTACKERS COULD DO...BEFORE THEY DO
imgflip.com

Security

Protection

Reputation



Using a Shift-Left Approach

Helps **prevent security vulnerabilities**, and protects your company's application, assets and reputation.

Integrate Threat Modelling into your projects to help drive a **Security First Culture** at your company.

Thank you

FLAGSTONE

FLAGSTONE

https://linktr.ee/Danielle.Dias