**Threat Modeling**

**Checklist**

Each of the overarching items need to be reviewed, but every item is not necessarily applicable. Based in part on the [OWASP Threat Modeling Cheatsheet](https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html).

A threat model should answer the following questions:

1. What is being built?
2. What can go wrong?
3. What is in place to prevent bad things?
4. Is it enough?

**System Design**

Review documentation or interview stakeholders for:

* Application Purpose
* Technology Stack
* Audience
* Roles

**Data Elements**

Possibilities may include:

* Financial Data
* Customer Private Information (PII)
* Intellectual Property
* Nonpublic Personal Information (NPI)
* Confidential Information
* Internal Use Only
* Public Information

**System Model**

Identify application and infrastructure architecture components and review for basic security provisioning

* Trust Boundaries
* Application Actors
* Data flows
* Data sources and sinks
* Information Elements (and classifications)
* Application Entry Points
* Servers
* Network Security Controls
* Containers

**Attack Types**

Utilizing Microsoft's STRIDE Model to classify possible attacks.

* Spoofing - Authenticity/Auditing
* Tampering - Integrity
* Repudiation - Non-repudiation/Auditing
* Information Disclosure - Confidentiality
* Denial of Service - Availability
* Elevation of Privilege - Authorization

**Possible Threat Agents**

Use the system model to identify possible threat agents, the following are just suggestions. Reduce this list to applicable threats for the system.

* Anonymous External Attacker (AEA)
* Anonymous Internal Attacker (AIA)
* Malicious Internal User (MIU)
* Malicious External User (MEU)
* Malicious Employee (ME)
* Malicious System Administrator (MSA)
* Malicious Developer (MD)
* Nation State Actor (NSA)

**Attacker Focused Matrix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **­Threat Agent** | **Asset** | **Attack** | **Attack Type** | **Goal** | **Impact** | **Mitigation** | **Finding** |
| AEA | Login Page | Brute-Forcing Attack | Spoofing | Access User Account | High: Exposure of Client Data and App Functionality | Authentication Controls | None |
| AIA | Registration Page | User Enumeration | Information Disclosure | Discover Confidential Information | Medium: Exposure of known user accounts | Out-of-band communication (email) | Flow validates the account |

**Process Focused Matrix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Goal** | **Asset** | **­Threat Agent** | **Attack** | **Attack Type** | **Impact** | **Mitigation** | **Finding** |
| Access User Account | Login Page | AEA | Brute-Forcing Attack | Spoofing | High: Exposure of Client Data and App Functionality | Authentication Controls | None |
| Discover Confidential Information | Registration Page | AIA | User Enumeration | Information Disclosure | Medium: Exposure of known user accounts | Out-of-band communication (email) | Flow validates the account |

**Asset Focused Matrix**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **­Threat Agent** | **Attack** | **Attack Type** | **Goal** | **Impact** | **Mitigation** | **Finding** |
| Login Page | AEA | Brute-Forcing Attack | Spoofing | Access User Account | High: Exposure of Client Data and App Functionality | Authentication Controls | None |
| Registration Page | AIA | User Enumeration | Information Disclosure | Discover Confidential Information | Medium: Exposure of known user accounts | Out-of-band communication (email) | Flow validates the account |