Threat Modelling Template

# Executive Summary

Use this section to provide a summary of what you were asked to review/assess and the specific risk concerns.

# Approach taken

This section should briefly set the scene on the modelling you will perform. Your approach (STRIDE, DREAD analysis, OWASP top10, etc) and any supporting documents should be referenced here.

# Business Architecture

This section should answer questions such as what does the business do? How does the business do it? What technologies are necessary for the business? What data flows in and out of the system? A diagram showcasing these in context is very helpful.

# Architecture decomposition

Here key elements such as trust boundaries, and identification of assets should be performed. It should show subsystems, authorization/authentication mechanisms, identify likely entry points, etc. Again, a diagram is very helpful.

# Threat identification

Identify your threats. These should be presented in tabular form, for example (non-prescriptive, other formats are available):

|  |  |
| --- | --- |
| Threat ID | Threat Identification and Title |
| Threat Agent | External, Internal, Lone individual, Criminal organisation, etc |
| Threat Description | Short description |
| Threat Target | Likely Target |
| Attack Surface | Point of entry |
| Attack Techniques | How the attack could be performed |
| Likelihood | A measure of the likelihood of the attack |
| Impact | A measure of the impact of a successful attack |
| Control | How can the attack be controlled |
| Mitigation | Mitigation techniques recommended |

Or any other suitable to your chosen approach

# Threat Rating / Risk assessment

A short description of your rating approach followed by a summary table with your risk assessment for each threat. Example, for STRIDE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Threats | **S**poofing Identity | **T**ampering | **R**epudiation | **I**nformation Disclosure | **D**enial of Service | **E**levation of Privilege |
| TA1 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TA2 |  |  |  |  |  |  |
| TA3 |  |  |  |  |  |  |
| TA4 |  |  |  |  |  |  |
| TA5 |  |  |  |  |  |  |
| TA6 |  |  |  |  |  |  |

And DREAD

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Threat | D | R | E | A | D | Total | Rating |
| TA1 | 3 | 3 | 3 | 3 | 3 | 15 | High |
| TA2 | 2 | 1 | 1 | 2 | 2 | 8 | Medium |
| TA3 | 1 | 1 | 1 | 0 | 0 | 3 | Low |
| TA4 |  |  |  |  |  |  |  |
| TA5 |  |  |  |  |  |  |  |
| TA6 |  |  |  |  |  |  |  |

Remember to include a definition for your range of values.

# Traceability/Compliance Matrix

Below is a Traceability Matrix, which is a brief summary of everything discussed in this document. (consider using a separate page in landscape mode for this)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Threat Agent** | **Asset** | **Attack** | **Attack Surface** | **Attack Goal** | **Impact** | **Control** | **Mitigation** |
| TA01 | A08 | SQL Injection | Login Form | User and System details | High: Access to personal user and system details | No whitelisting or prepared statements are in place to stop this | Primary Defences:  Option 1: Use of Prepared Statements  Option 2: Use of Stored Procedures  Option 3: Allow-list Input Validation  Option 4: Escaping All User Supplied Input |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Conclusion

Your conclusions drawn from the threat modelling performed addressing any recommendations to the developer team,identifying areas of concern to draw immediate attention and other recommendations.

# References

List of references used.

Some supporting documents you can use

OWASP Cheat Sheets (2021) <https://github.com/OWASP/CheatSheetSeries/tree/master/cheatsheets>

Meier et all (2005A) *How To: Create a Threat Model for a Web Application at Design Time* retrieved from Microsoft Corporation <https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff647894(v=pandp.10)?redirectedfrom=MSDN>

Meier et all (2005B) *Template: Web Application Threat Model* retrieved from Microsoft Corporation <https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648866(v=pandp.10)?redirectedfrom=MSDN>

Meier et all (2005C) *Cheat Sheet: Web Application Security Frame* retrieved from Microsoft Corporation <https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649461(v=pandp.10)?redirectedfrom=MSDN>

Meier et all (2005D) *Threat Modeling Web Applications* retrieved from Microsoft Corporation <https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648006(v=pandp.10)?redirectedfrom=MSDN>

Referencing@Portsmouth (N.b) retrieved from Portsmouth University, The University Library <http://referencing.port.ac.uk>