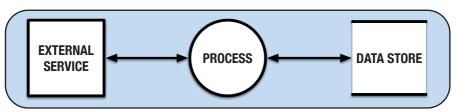


https://threatmodel.co.uk



S poofing	Authentication	Fraudulent Data Impersonating legitimate Users Pretending to be something it isn't
T ampering	Integrity	Unauthorised changes to Data Man-In-The-Middle (MITM) Interfering with Data Integrity
R epudiation	Non-Repudiation	Is there an Audit Trail? Can an Attacker hide their activity? Prevented logging of user actions
nformation	Confidentiality	Data transmitted un-encrypted Leaking of Personal Data (PII) Inadequete Access Control List (ACL)
Denial	Availability	Inaccessbile products or services Resource exhaustion Reduced performance
E levation	Authorisation	Bugs, exploits and misconfiguration increas- ing a user's access level Users being able to access services or resources which they shouldn't

Low 3 Medium 6 High 8 Critical 10		
D amage	How much damage would this vulnerability cause if exploited?	How bad would an attack be? From the Business and Service perspectives
R eproducability	How difficult is it to reproduce this vulnerability?	How easy is it to reproduce? Is it predictable or unpredictable? Are there other factors required?
E xploitability	How easy is it to exploit?	How easy is it to exploit? Is exploiting simple or complex? Requires multiple vulnerabilities?
Affected	Who is affected?	How many users will it impact? Does it affect only service users?
D iscoverability	How difficult is it to discover this vulnerability?	How easy is it to discover the vulnerability? Exposed configuration information