Week-01 OWASP Rating Methodology

1. **Explain the two sets of Factors - Threat Agents and Vulnerability**

Risiko = sandsynlighed ∗ påvirkning

Threat Agents:

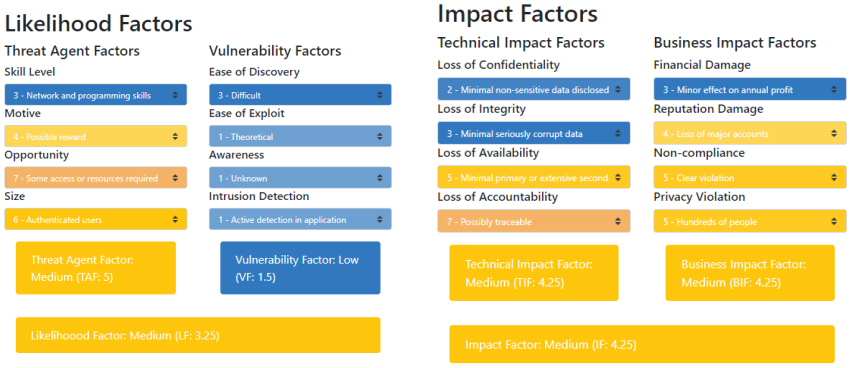
Threat Agents er individer eller grupper der forsøger / vil forsøge et angreb på systemet.

- Færdighed - Hvor teknisk dygtige er agenterne.
- Motiv - Hvor motiveret er gruppen for at finde og udnytte sårbarheder.
- Mulighed - Hvor mange ressourcer og hvad for nogle muligheder skal agenterne have for at kunne udnytte sårbarheden.
- Størrelse - Hvor stor er gruppen.

Vulnerability:

Selve sårbarheden.

- Opdagelse - Hvor nemt er det for gruppen at opdage sårbarheden.
- Udnyttelse - Hvor nemt er det for gruppen at udnytte sårbarheden.
- Opmærksom - Hvor velkendt er sårbarheden?
- Afsløring - Hvor sandsynligt er det at blive opdaget for at udnytte sårbarheden.



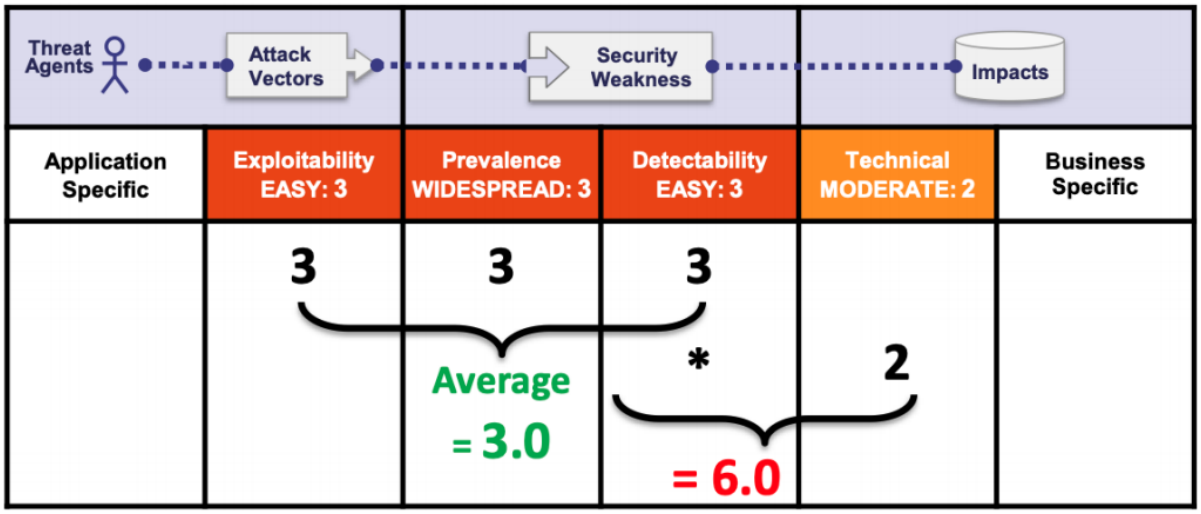
2. Give some examples of how you can change those parameters - for example for MySQL servers

Brug juiceshop login page og skriv ‘ for at ændre på discovery og exploitability.
Man vil ikke have at exceptions er tilgængelige for brugere.


```
{
  "error": {
    "message": "SQLITE_ERROR: near \"' AND password = '\": syntax error",
    "stack": "SequelizeDatabaseError: SQLITE_ERROR: near \"' AND password = '\": syntax error\n    at Query.formatError (C:\\Users\\Asger\\Doc
    "name": "SequelizeDatabaseError",
    "parent": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Users WHERE email = '\"Hans' or 1=1' AND password = '202cb962ac59075b964b07152d234b70' AND deletedAt IS NULL"
    },
    "original": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Users WHERE email = '\"Hans' or 1=1' AND password = '202cb962ac59075b964b07152d234b70' AND deletedAt IS NULL"
    },
    "sql": "SELECT * FROM Users WHERE email = '\"Hans' or 1=1' AND password = '202cb962ac59075b964b07152d234b70' AND deletedAt IS NULL"
  }
}
```

3. Explain how security risks are rated in OWASP

(exploitability + prevalence + detectability) / 3 * technical



4. Argue whether OWASP gives the complete picture of security risks on an application

Den giver ikke det fulde overblik over alle sikkerhedsrisici der findes eller kommer til at findes, men det giver en top 10 liste af de mest farlige og mulige angreb man kan udsættes for.

RISK	Threat Agents	Attack Vectors: Exploitability	Security Weakness: Prevalence	Security Weakness: Detectability	Impacts: Technical	Impacts: Business	Score
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0