List of Worst and/or Broken Passwords

- How many lists of Worst Passwords can you find via Google
  - Nordpass.com has the top 200 of worst password listed[1]
    "The most popular passwords contain all the obvious and easy to guess number combinations (12345,111111,123321), popular female names (Nicole, Jessica, Hannah), and just strings of letters forming a horizontal or vertical line on a QWERTY keyboard (asdfghjkl, qazwsx, 1qaz2wsx, etc.). Surprisingly, the most obvious one — "password" — remains very popular; 830,846 people still use it." - ***Nordpass.com***

- How many lists of possible valid usernames/passwords can you find via Google
  - Lifehacker got a top 10 of possible usernames/passwords which were listed in possibility of validation[2]

Preventing bad passwords

- Why is this not always as easy as it sounds? - which two "project requirements" often draws in two quite different directions?
  - Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential reuse attacks.
  - Do not ship or deploy with any default credentials, particularly for admin users.
  - Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.
  - Align password length, complexity and rotation policies with NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence based password policies.
  - Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.
  - Limit or increasingly delay failed login attempts. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.
  - Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.
- Implement a simple control (feel free to use predefined packages) to verify passwords, up against a set of rules decided by you (length, required character, illegal words etc.)
  - **Rules**
    - min 8 characters
    - must have at least 1 Uppercase letter,
    - 1 number, and
    - 1 special character
    - must not contain any words in your email/username

[1] https://nordpass.com/blog/top-worst-passwords-2019/
[2] https://lifehacker.com/the-top-10-usernames-and-passwords-hackers-try-to-get-i-1762638243

- OWASP Risk Rating Methodology
    - We need information about
        - the threat agent involved,
        - the attack that will be used,
        - the vulnerability involved, and
        - the impact of a successful exploit on the business
    - risk = likelihood $*$ impact

- Explain the two sets of Factors - Threat Agents and Vulnerability

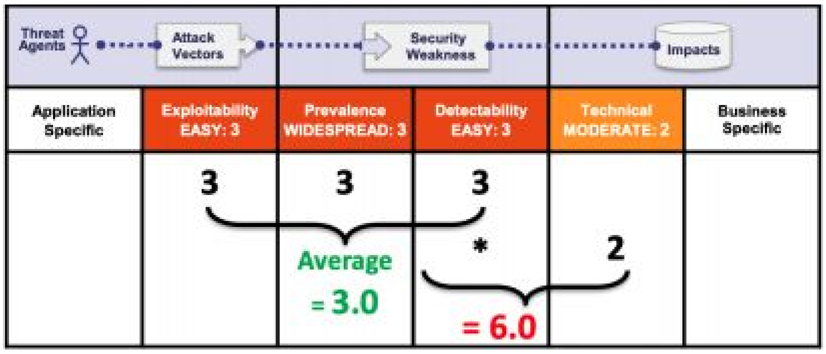
  Threat Agents

  - Skill level. How technically skilled is this group of threat agents?
    - Security penetration skills (9), network and programming skills (6), advanced computer user (5), some technical skills (3), no technical skills (1)
  - Motive. How motivated is this group of threat agents to find and exploit this vulnerability?
    - Low or no reward (1), possible reward (4), high reward (9)
  - Opportunity. What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability?
    - Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
  - Size. How large is this group of threat agents?
    - Developers (2), system administrators (2), intranet users (4)

  Vulnerability

  - Ease of discovery. How easy is it for this group of threat agents to discover this vulnerability?
    - Practically impossible (1), difficult (3), easy (7), automated tools available (9)
  - Ease of exploit. How easy is it for this group of threat agents to actually exploit this vulnerability?
    - Theoretical (1), difficult (3), easy (5), automated tools available (9)
  - Awareness. How well known is this vulnerability to this group of threat agents?
    - Unknown (1), hidden (4), obvious (6), public knowledge (9)
  - Intrusion detection. How likely is an exploit to be detected?
    - Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

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

- Explain how security risks are rated in OWASP
    - 

Threat Agents	Attack Vectors	Security Weakness		Impacts	
Application Specific	Exploitability EASY: 3	Prevalence WIDESPREAD: 3	Detectability EASY: 3	Technical MODERATE: 2	Business Specific
	3	3	3	2	

- Argue whether OWASP gives the complete picture of security risks on an application
    - OWASP does give the full picture of security risks on a application, though we only go over some of the top 10 vulnerabilities.
    - link to all risks here