Authentication Flaws

❌ Typical Flaws in Authentication

- Permits brute force or other automated attacks
- Permits default, weak, or well-known passwords
- Uses weak or ineffective credential recovery and forgot-password processes (e.g. "knowledge-based answers")
- Uses plain text, encrypted, or weakly hashed passwords
- Has missing or ineffective multi-factor authentication
- Exposes Session IDs in the URL
- Does not rotate Session IDs after successful login
- Does not properly invalidate Session IDs

Risk Rating

Broken Authentication

Exploitability	Prevalence	Detecability	Impact	Risk
🔴 Easy	🔶 Common	🔶 Average	🔴 Severe	A2
(3	+ 2	+ 2) / 3	* 3	= 7.0

Exercise

1. Watch How To Keep Your Passwords Safe 📺
2. Log in with MC SafeSearch's user account (⭐⭐)

Password Strength Controls

- **Enforce minimum password length** of at least 10 characters
- Maximum length should allow 64 characters or more
- **No periodic password resets** as users rely on predictable patterns
- Avoid password complexity rules as *all of them* are predictable
- Ban bad passwords or ones which have appeared in data breaches
  - e.g. Troy Hunt's 10GB+ list or Daniel Miesler's various lists
- Allow convenience features on password fields
  - Offer *Show Password while typing* option
  - Allow pasting from clipboard into password fields

Other Authentication Controls

- **Transmit passwords only over TLS**
  - The "login landing page" must be served over TLS as well
- **Prevent Brute-Force Attacks** (e.g. throttling or periodic lockout)
- Require re-authentication for sensitive features
- **Offer optional 2FA / MFA**
  - Consider strong transaction authentication

Enterprise Controls

- Use centralized corporate authentication system (if in place)

Exercise

1. Log in as admin exploiting its insufficient *Password Strength* (★★)
2. *Reset Jim's Password* by answering his secret question (★★★)
3. *Login Bjoern* using his Gmail account (★★★★)