

# 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 (⭐⭐)

⚠️ *Do **not** use SQL Injection for authentication bypass!*

# Exercise

1. Pick one Security Question and explain how 💪 it is against attacks.
2. What would you recommend to pick as an answer? Assume that the risk of compromise is full takeover of your user account.

**Security Question** ⚠️ This cannot be changed later!

Your eldest siblings middle name?  
Mother's maiden name?  
Mother's birth date? (MM/DD/YY)  
Father's birth date? (MM/DD/YY)  
Maternal grandmother's first name?  
Paternal grandmother's first name?  
Name of your favorite pet?  
Last name of dentist when you were a teenager? (Do not include 'Dr.')  
Your ZIP/postal code when you were a teenager?  
Company you first work for as an adult?

## 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)









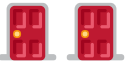
# Two-Factor Authentication

Two-factor authentication adds a second level of authentication to an account log-in. When you have to enter only your username and one password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:

- **Something you know**, such as a personal identification number (PIN), password or a pattern
- **Something you have**, such as an ATM card, phone, or fob
- **Something you are**, such as a biometric like a fingerprint or voice print [<sup>1</sup>]






## 2FA Method Comparison

Method	Security	Privacy	Access
SMS			
Authenticator App			
Hardware Key			

Hardware keys win from a security perspective, they are private and unaffected by a dying or out of range phone. However, only a few services (Google, Dropbox, Facebook, Github and a few others) support the standard so far. Unless you trust your phone provider (and few providers are trustworthy), **an authenticator app is the best option.**

# Password Managers

Password managers are programs, browser plugins or web services that automate management of large number of different credentials, including memorizing and filling-in, generating random passwords on different sites etc. [<sup>2</sup>]

 KeePass		
Open Source (GPLv2)	Proprietary / Freemium	Proprietary
Local installation, optional file or cloud sync	Cloud-based	Local installation with Cloud sync

# Exercise

1. Log in with the admin's user account (★ ★)
2. Reset Jim's password by answering his secret question (★ ★ ★)
3. Log in with Bjoern's user account (★ ★ ★ ★)