



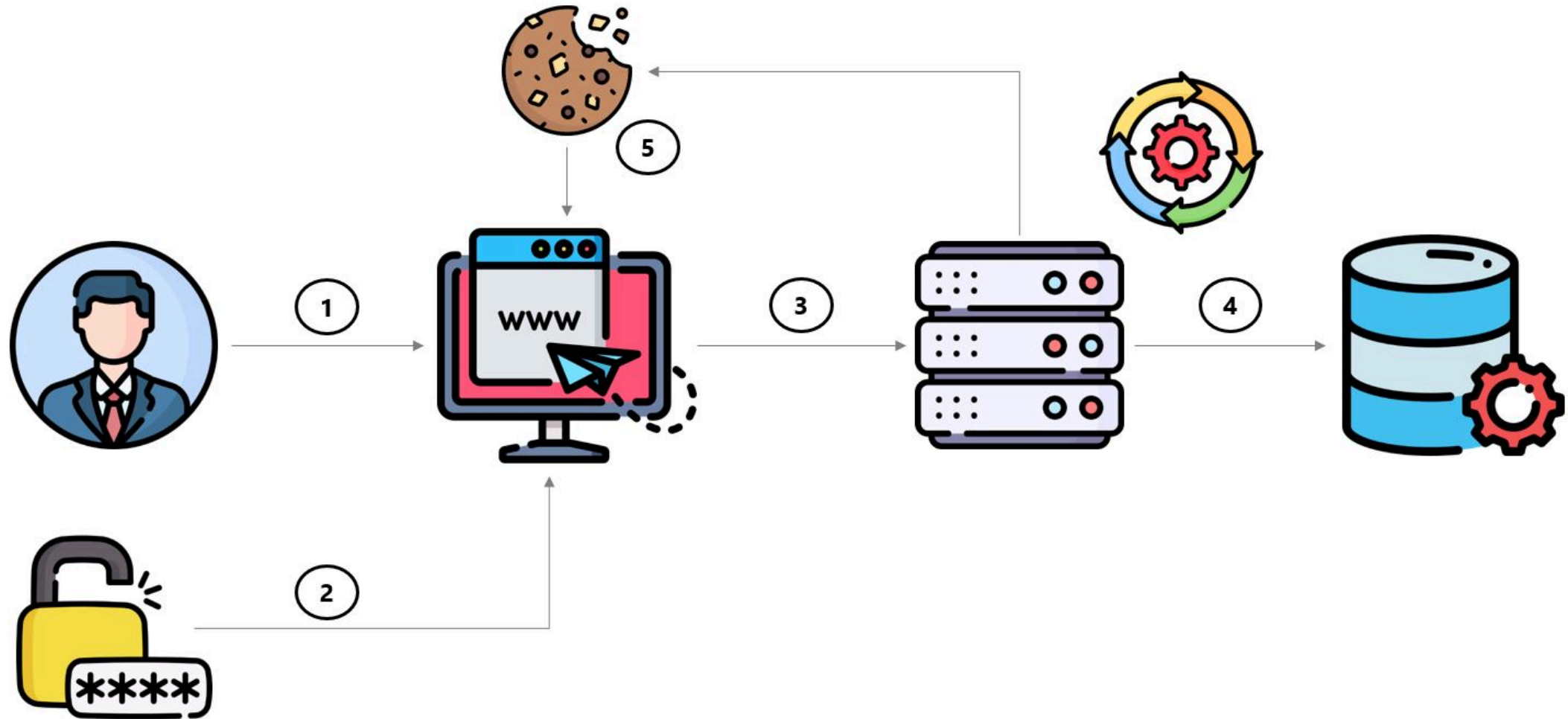


Authentication Flaws

Authentication

-  Who are you
-  Verify the user's identity
-  Authentication works through password, one time pins, biometric information
-  Usually done before authorization

Website authentication - Server Session



✗ 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






Data Factors

A07:2021 – Identification and Authentication Failures

CWEs Mapped	Max Incidence Rate	Avg Incidence Rate	Avg Weighted Exploit	Avg Weighted Impact	Max Coverage	Avg Coverage	Total Occurrences	Total CVEs
22	14.84%	2.55%	7.40	6.50	79.51%	45.72%	132,195	3,897

Exercise 4.1 ()

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 4.2 (📌)

1. What benefits and downsides (if any) would enforcing user passwords with the advice below have?
2. What password might the user currently have typed in?

The image shows a dark-themed password form. At the top is a 'Password' input field with five dots. Below it is a hint: 'Password must be 5-20 characters long.' with a character count of '5/20'. Below that is a 'Repeat Password' input field, also with five dots and a '5/20' character count. A toggle switch labeled 'Show password advice' is turned on. Below the toggle is a list of five password requirements, each with an icon: a red exclamation mark for the first four and a blue checkmark for the third.

Password

Password must be 5-20 characters long. 5/20

Repeat Password

5/20

☒ Show password advice

- ❗ contains at least one lower character
- ❗ contains at least one upper character
- ✓ contains at least one digit
- ❗ contains at least one special character
- ❗ contains at least 8 characters

Exercise 4.3 (📌)

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?



Prevention



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

Secure "Forgot Password" Mechanism

- Return a consistent message for both existent and non-existent accounts
- Ensure that the time taken for the user response message is uniform
- Use a side-channel to communicate the method to reset their password
- Use URL tokens for the simplest and fastest implementation
- Ensure that generated tokens or codes are:
 - Randomly generated using a cryptographically safe algorithm
 - Sufficiently long to protect against brute-force attacks
 - Stored securely
 - Single use and expire after an appropriate period

Secure Password Storage

- Use [Argon2id](#) unless you have a good reason not to
- Set a reasonable [work factor](#) for your system
- Use a [salt](#) (modern algorithms like Argon2id, bcrypt and PBKDF2 do this for you automatically)
- Consider using a [pepper](#) to provide an additional layer of security

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) 100

➡ Two-Factor Authentication

Two-factor authentication adds a second level of authentication to an account login. 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 [¹]


2FA Method Comparison

Method	Security	Privacy	Access	Prevalence
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.

 KeePass	LastPass ...	1Password
Open Source (GPLv2)	Proprietary / Freemium	Proprietary
Local installation, optional file or cloud sync	Cloud-based	Local installation with Cloud sync



More web

Web applications should at least not make password managers job more difficult than necessary by observing the following recommendations:

- use standard HTML forms for username and password input with appropriate `type` attributes,
- do not artificially limit user passwords to a length "reasonable for humans" and allow passwords lengths up to 128 characters,
- do not artificially prevent copy and paste on username and password fields,
- avoid plugin-based login pages (Flash, Silverlight etc) [¹]

Exercise 4.4 (🏠)

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 Google account (★ ★ ★ ★)

⚠️ *Do **not** use SQL Injection for authentication bypass! Also, do **not** hack Bjoern's actual Google account!*

Exercise 4.5 (*optional*)

1. Install a 2FA app on your phone (e.g. [Google Authenticator](#) or [Authy](#))
2. Visit <https://2fa.directory/> and find out what services you use offer 2FA
3. Turn 2FA on wherever possible
4. Do not forget to print (= 🖨️!) the backup codes and keep them safe

💡 *Pro tip: Print hard copies of the originally displayed QR codes for easy setup on any new phone! Just store them very securely!*