LAB 01 report

1. Search Results

When I searched for my name using the Brave browser in incognito mode, I came across only a few general results that didn't contain any direct personal information.

However, searching with Google Chrome brought up several sources of personal data, such as:

- My Instagram and Facebook profiles.
- My bibliography entry on the COBISS portal
- News articles and local posts about my karate achievements.
- Mentions of my bachelor's work.
- Some photos of me

This shows that Chrome, because it personalizes results based on my Google account history—reveals significantly more personal information than the privacy-focused Brave browser.

2. Exposure Check

When I checked my email using HaveIBeenPwned, I found that it was involved in several older data breaches tied to outdated online accounts.

There were no active or recent leaks, but the presence in past breaches suggests that some of my old credentials may have been exposed.

3. Potential Risks

Publicly available information could lead to the following risks:

- Profiling: Personal details, interests, and academic background could be used to build a detailed profile of me.
- Impersonation or identity theft: Someone could use my photos or social media content to create fake profiles.
- Phishing: Exposed email addresses could be exploited for scams.
- Reputational risk: Older photos or public mentions might be taken out of context.

4. Worst-Case Scenario

In the worst-case scenario, someone could gather my name, photos, and social media profiles to create a fake identity.

They could then:

- Contact my friends or coworkers, pretending to be me, to ask for money or personal information
- Spread misinformation or damage my online reputation
- Combine old breach data with my current information to hack into my accounts

5. Personal Security and Privacy Rating

I'd rate my privacy and security at 3.5 out of 5.

I use strong passwords and two-factor authentication.

My social media privacy settings are moderate.

However, some personal data and photos are still visible through Google searches, and a few older credentials were part of past breaches.

6. Recommendations

- Regularly monitor data exposure using tools like HaveIBeenPwned
- Remove or limit public visibility of personal info on social media
- Use privacy-oriented browsers like Brave or Firefox, and clear cookies before searching
- Update or delete old accounts linked to breaches
- Enable two-factor authentication on all important accounts