UPB  
Zadanie 3 – Autentifikácia

Riešitelia: Emília Čurillová, Filip Harvančík, Lenka Puškášová

**Úloha1 (Lenka)**

* **Kontrola kompromitácie hesla:** Pri registrácii sa heslo lokálne hashuje pomocou SHA-1 a pošle sa len prvých 5 znakov hashu na HIBP (Have i been pwned) range API (https://api.pwnedpasswords.com/range/{prefix}). API vráti zoznam zvyšných suffixov a počty výskytov; ak sa lokálny suffix zhoduje s niektorým z odpovede, heslo je kompromitované a odmietne sa. Tento prístup používa **k-anonymitu**, takže server HIBP nikdy nevidí celé heslo ani celý hash
* **Komplexita** –
  + komplexita hesiel nebude kontrolovaná – uživatelia majú tendenciu vymýšľať viac predikovateľné heslá ak sú nútení držať sa LUDS odporúčania – vtedy bude minimálna dĺžka 15
  + komplexita sa bude držať LUDS composition policy, vtedy bude minimálna dĺžka hesla 8
* Heslo sa moze nachadzat v db len raz – bude implementovane v ulohe dva s vyuzitim saltu

Zdroje

Odporúčania pre dĺžku a komplexitu hesla  
<https://www.strongdm.com/blog/nist-password-guidelines>

API pre kompromitovane hesla  
<https://haveibeenpwned.com/api/v3#:~:text=stealer%20logs%20APIs.-,Pwned%20Passwords,-Overview>

**Úloha2 ()**

**Úloha 3 ()**

**Úloha 4 ()**